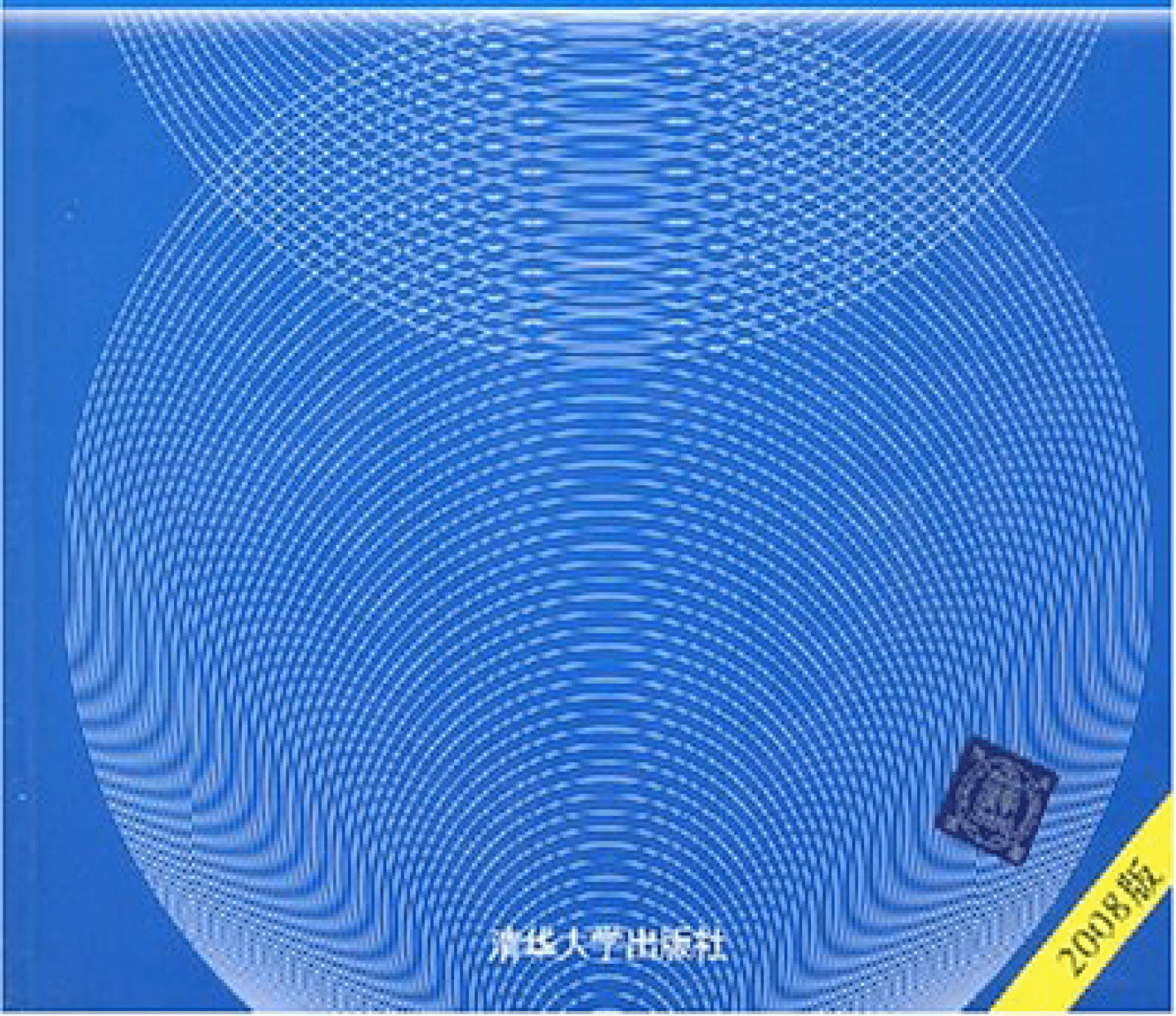
全国计算机技术与软件专业技术资格（水平）考试指定用书

网络管理员教程

（第2版）

张国鸣 严体华 主编
全国计算机技术与软件专业技术资格（水平）考试办公室组编



清华大学出版社

全国计算机技术与软件专业技术资格(水平)考试指定用书

网络管理员教程

(第 2 版)

全国计算机技术与软件专业技术资格(水平)考试办公室组编
张国鸣　严体华　主编

清华大学出版社
北　京

内 容 简 介

本书按照人事部、信息产业部全国计算机技术与软件专业技术资格(水平)考试要求编写,内容紧扣《网络管理员考试大纲》。全书共分8章,分别对计算机网络基本概念、因特网及其应用、局域网技术与综合布线、网络操作系统、应用服务器配置、Web网站建设、网络安全和网络管理进行了系统讲解。

本书层次清晰、内容丰富,注重理论与实践相结合,力求反映计算机网络技术的最新发展,既可作为网络管理员资格考试的教材,也可作为网络与通信技术基础各类培训的教材,同时也可供计算机网络工程及管理人员自学使用。

图书在版编目(CIP)数据

网络管理员教程/张国鸣,严体华主编.—2版.—北京:清华大学出版社,2006.6

(全国计算机技术与软件专业技术资格(水平)考试指定用书)

ISBN 7-302-12958-4

Ⅰ.网…　Ⅱ.①张…②严…　Ⅲ.计算机网络－工程技术人员－资格考核－教材　Ⅳ.TP393

中国版本图书馆CIP数据核字(2006)第043276号

出 版 者: 清华大学出版社　　**地　　址:** 北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编:** 100084

社 总 机: 010-62770175　　**客户服务:** 010-62776969

组稿编辑: 柴文强

文稿编辑: 刘　霞

印 刷 者: 清华大学印刷厂

装 订 者: 三河市化甲屯小学装订二厂

发 行 者: 新华书店总店北京发行所

开　　本: 185×230　**印张:** 31.75　**防伪页:** 1　**字数:** 711千字

版　　次: 2006年6月第2版　2006年6月第1次印刷

书　　号: ISBN 7-302-12958-4/TP・8236

印　　数: 1～20000

定　　价: 50.00元

序

在国务院鼓励软件产业发展政策的带动下，我国软件业一年一大步，实现了跨越式发展，销售收入由2000年的593亿元增加到2003年的1633亿元，年均增长速度39.2%；2000年出口软件仅4亿美元，去年则达到20亿美元，三年中翻了两番多；全国“双软认证工作体系”已经规范运行，截止2003年11月底，认定软件企业8582家，登记软件产品18 287个；11个国家级软件产业基地快速成长，相关政策措施正在落实；我国软件产业的国际竞争力日益提高。

在软件产业快速发展的带动下，人才需求日益迫切，队伍建设与时俱进，而作为规范软件专业人员技术资格的计算机软件考试已在我国实施了十余年，累计报考人数超过一百万，为推动我国软件产业的发展作出了重要贡献。

软件考试在全国率先执行了以考代评的政策，取得了良好的效果。为贯彻落实国务院颁布的《振兴软件产业行动纲要》和国家职业资格证书制度，国家人事部和信息产业部对计算机软件考试政策进行了重大改革：考试名称调整为计算机技术与软件专业技术资格（水平）考试；考试对象从狭义的计算机软件扩大到广义的计算机软件，涵盖了计算机技术与软件的各个主要领域（5个专业类别、3个级别层次和20个职业岗位资格）；资格考试和水平考试合并，采用水平考试的形式（与国家接轨，报考不限学历与资历条件），执行资格考试政策（各用人单位可以从考试合格者中择优聘任专业技术职务）；这是我国人事制度改革的一次新突破。此外，将资格考试政策延伸到高级资格，使考试制度更为完善。

信息技术发展快，更新快，要求从业人员不断适应和跟进技术的变化，有鉴于此，国家人事部和信息产业部规定对通过考试获得的资格（水平）证书实行每隔三年进行登记的制度，以鼓励和促进专业人员不断接受新知识、新技术、新法规的继续教育。考试设置的专业类别、职业岗位也将随着国民经济与社会发展而动态调整。

目前，我国计算机软件考试的部分级别已与日本信息处理工程师考试的相应级别实现了互认，以后还将继续扩大考试互认的级别和国家。

为规范培训和考试工作，信息产业部电子教育中心组织一批具有较高理论水平和丰富实践经验的专家编写了全国计算机技术与软件专业技术资格（水平）考试的教材和辅导用书，按照考试大纲的要求，全面介绍相关知识与技术，帮助考生学习和备考。

我们相信，经过全社会的共同努力，全国计算机技术与软件专业技术资格（水平）考试将会更加规范、科学，进而对培养信息技术人才，加快专业队伍建设，推动国民经济和社会信息化作出更大的贡献。

信息产业部副部长　娄勤俭

前　言

（第 2 版）

全国计算机软件考试实施至今已经历了十多年，在社会上产生了很大影响，对我国软件产业的形成和发展做出了重要贡献。随着因特网的迅猛发展，电子政务和电子商务的快速兴起，人类正在以前所未有的速度跨入信息化社会，进入网络时代。计算机网络越来越成为人类各种活动中必不可少的一部分，成为政府施政、企业管理、商家经营的主要平台，成为人与人之间进行沟通交流的重要形式。为了适应我国信息化发展的需求，国家人事部和信息产业部决定将考试的级别拓展到计算机与软件技术的各个方面，增设了网络管理员级别考试，以满足社会对各种信息技术人才的需要。

编者受全国计算机技术与软件专业技术资格（水平）考试办公室委托，编写《网络管理员教程》一书，以适应网络管理员级别考试大纲的要求。编者在撰写本书时紧扣《网络管理员考试大纲》，对考生需要掌握的内容进行了全面、深入的阐述。全书共分 8 章，分别对计算机网络基本概念、Internet 及其应用、局域网技术与综合布线、网络操作系统、应用服务器配置、Web 网站建设、网络安全和网络管理进行了系统讲解。需要指出的是，计算机网络管理既具有较强的理论性，又是一门实践性很强的技术。所以，希望读者在学习过程中要注重理论与实践相结合。本书是全国计算机技术与软件专业技术资格（水平）考试网络管理员教材，同时也可作为初级网络管理工程技术人员的参考书。

本书由张国鸣、严体华主编，第 1 章和第 2 章由曲振英编写，第 3 章由崔景俐编写，第 4 章和第 5 章由严体华、贺唯佳编写，第 6 章由黄健斌编写，第 7 章由查正朋编写，第 8 章由唐树才编写。自 2004 年 7 月出版第 1 版以来，先后进行了 5 次印刷，共印 54000 册。编者再版时，遵循“概念清晰、内容新颖、通俗易懂、实用性强”的原则，积极吸纳读者提出的意见和建议，重点对网络操作系统、应用服务器配置、网络安全和网络管理等章节的内容进行了相应调整。在此对热心读者提出的宝贵意见表示衷心感谢，同时也欢迎广大读者对再版内容进行批评指正。

编　者

2006 年 5 月

目　录

第1章 计算机网络概述

1.1 数据通信基础

1.1.1 数据通信的基本概念

1. 数据信号

数据可分为模拟数据与数字数据两种。在通信系统中，表示模拟数据的信号称作模拟信号，表示数字数据的信号称作数字信号，二者是可以相互转化的。模拟信号在时间上和幅度取值上都是连续的，其电平随时间连续变化，如图1-1(a)所示。例如，语音是典型的模拟信号，其他由模拟传感器接收到的信号如温度、压力、流量等也是模拟信号。数字信号在时间上是离散的，在幅值上是经过量化的，它一般是由二进制代码0、1组成的数字序列，如图1-1(b)所示。例如，计算机中传送的是典型的数字信号。

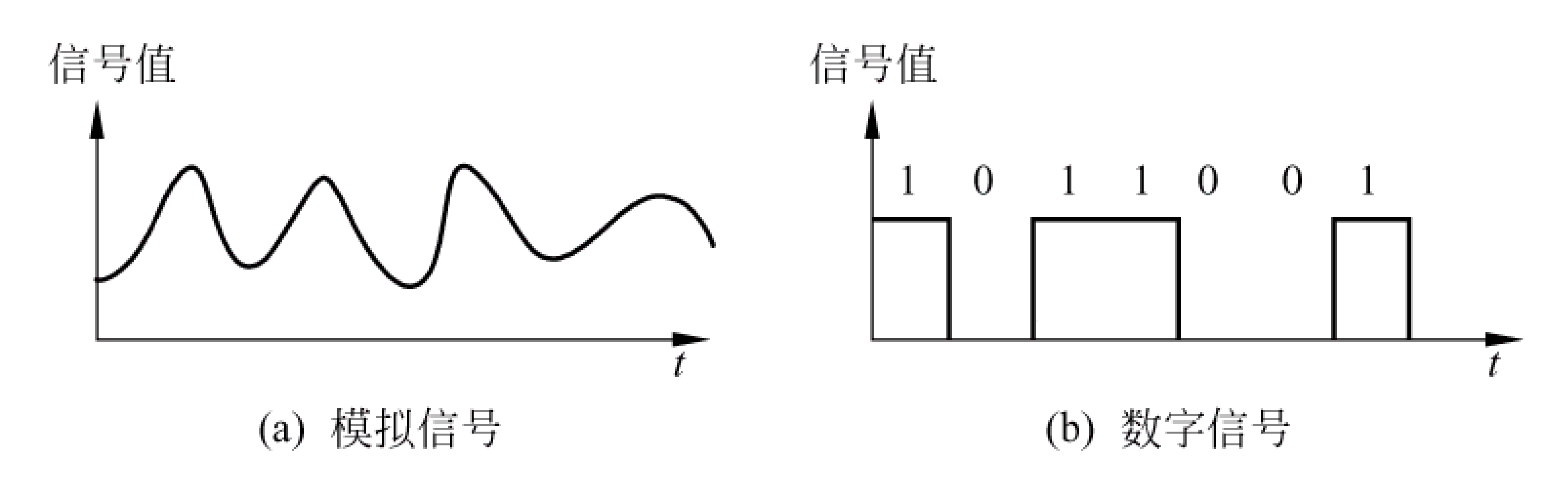
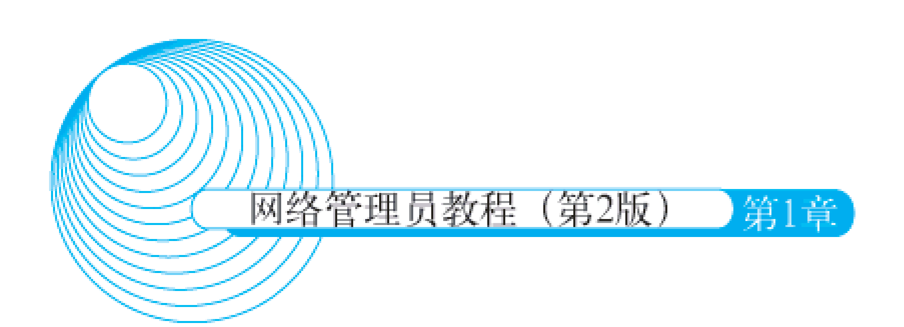


图1-1 模拟信号和数字信号

传统的电话通信信道是传输音频的模拟信道，无法直接传输计算机中的数字信号。为了利用现有的模拟线路传输数字信号，必须将数字信号转化为模拟信号，这一过程称作调制(Modulation)。在另一端，接受到的模拟信号要还原成数字信号，这个过程称作解调(Demodulation)。通常由于数据的传输是双向的，因此，每端都需要调制和解调，这种设备称作调制解调器(Modem)。

模拟信号的数字化需要3个步骤：采样、量化和编码。采样是指用每隔一定时间的信号样值序列来代替原来在时间上连续的信号，也就是在时间上将模拟信号离散化。量化是用有限个幅度值近似原来连续变化的幅度值，把模拟信号的连续幅度变为有限数量的有一定间隔的离散值。编码则是按照一定的规律，把量化后的值用二进制数字表示，然后转换成二值或多值的数



字信号流，这样得到的数字信号可以通过电缆、光纤、微波干线、卫星通道等数字线路传输，在接收端则与上述模拟信号数字化过程相反，经过滤波又恢复成原来的模拟信号，上述数字化的过程又称为脉冲编码调制。

2. 信道

要进行数据终端设备之间的通信当然要有传输电磁波信号的电路，这里所说的电路既包括有线电路，也包括无线电路。信息传输的必经之路称为“信道”。信道有物理信道和逻辑信道之分。物理信道是指用来传送信号或数据的物理通路，网络中两个节点之间的物理通路称为通信链路，物理信道由传输介质及有关设备组成。逻辑信道也是一种通路，但在信号收、发点之间并不存在一条物理上的传输介质，而是在物理信道基础上，由节点内部或节点之间建立的连接来实现的。通常把逻辑信道称为“连接”。

信道和电路不同，信道一般都是用来表示向某一个方向传送数据的媒体，一个信道可以看成是电路的逻辑部件，而一条电路至少包含一条发送信道或一条接收信道。

3. 数据通信模型

图 1-2 所示的是数据通信系统的基本模型。远端的数据终端设备(DTE，Data Terminal Equipment)通过数据电路与计算机系统相连。数据电路由通信信道和数据通信设备(DCE，Data Communication Equipment)组成。如果通信信道是模拟信道，DCE 的作用就是把 DTE 送来的数据信号变换为模拟信号再送往信道，信号到达目的节点后，把信道送来的模拟信号变换成数据信号再送到 DTE；如果通信信道是数字信道，DCE 的作用就是实现信号码型与电平的转换、信道特性的均衡、收发时钟的形成与供给以及线路接续控制等。

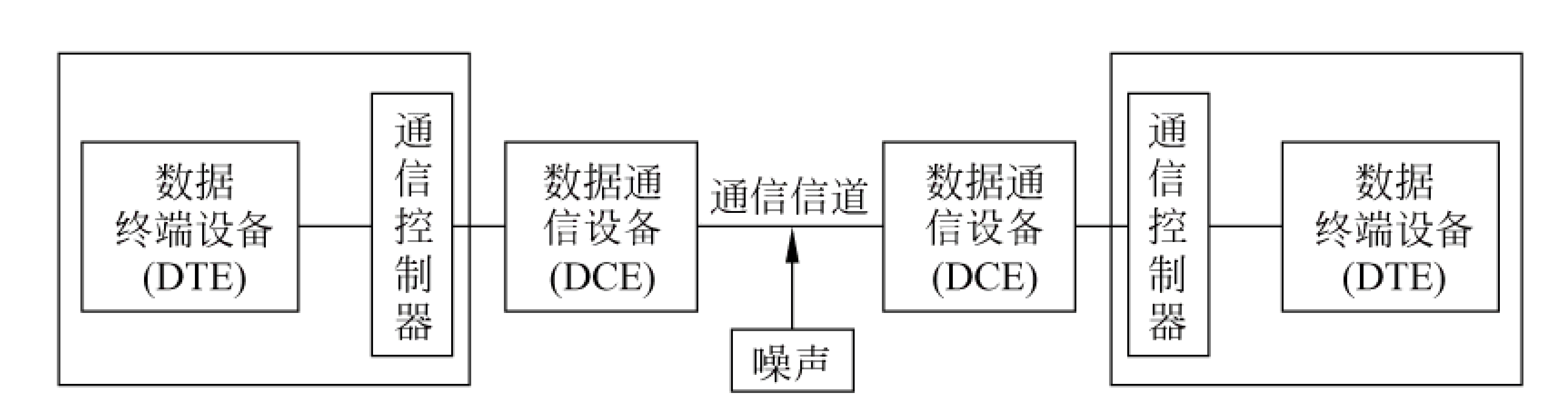


图 1-2　数据通信模型

数据通信和传统的电话通信的重要区别之一是，电话通信必须有人直接参加，摘机拨号，接通线路，双方都确认后才开始通话。在通话过程中有听不清楚的地方还可要求对方再讲一遍。在数据通信中也必须解决类似的问题，才能进行有效的通信。但由于数据通信没有人直接参加，就必须对传输过程按一定的规程进行控制，以便使双方能协调可靠地工作，包括通信线路的连接，收发双方的同步，工作方式的选择，传输差错的检测与校正，数据流的控制，数据交换过程

中可能出现的异常情况的检测和恢复，这些都是按双方事先约定的传输控制规程来完成的，具体工作由图 1-2 中的通信控制器来完成。

4. 数据通信方式

根据所允许的传输方向，数据通信方式可分成以下 3 种。

（1）单工通信：数据只能沿一个固定方向传输，即传输是单向的。如图 1-3(a)所示。

（2）半双工通信：允许数据沿两个方向传输，但在任一时刻信息只能在一个方向传输。如图 1-3(b)所示。

（3）双工通信：允许信息同时沿两个方向传输，这是计算机通信常用的方式，可大大提高传输速率。如图 1-3(c)所示。

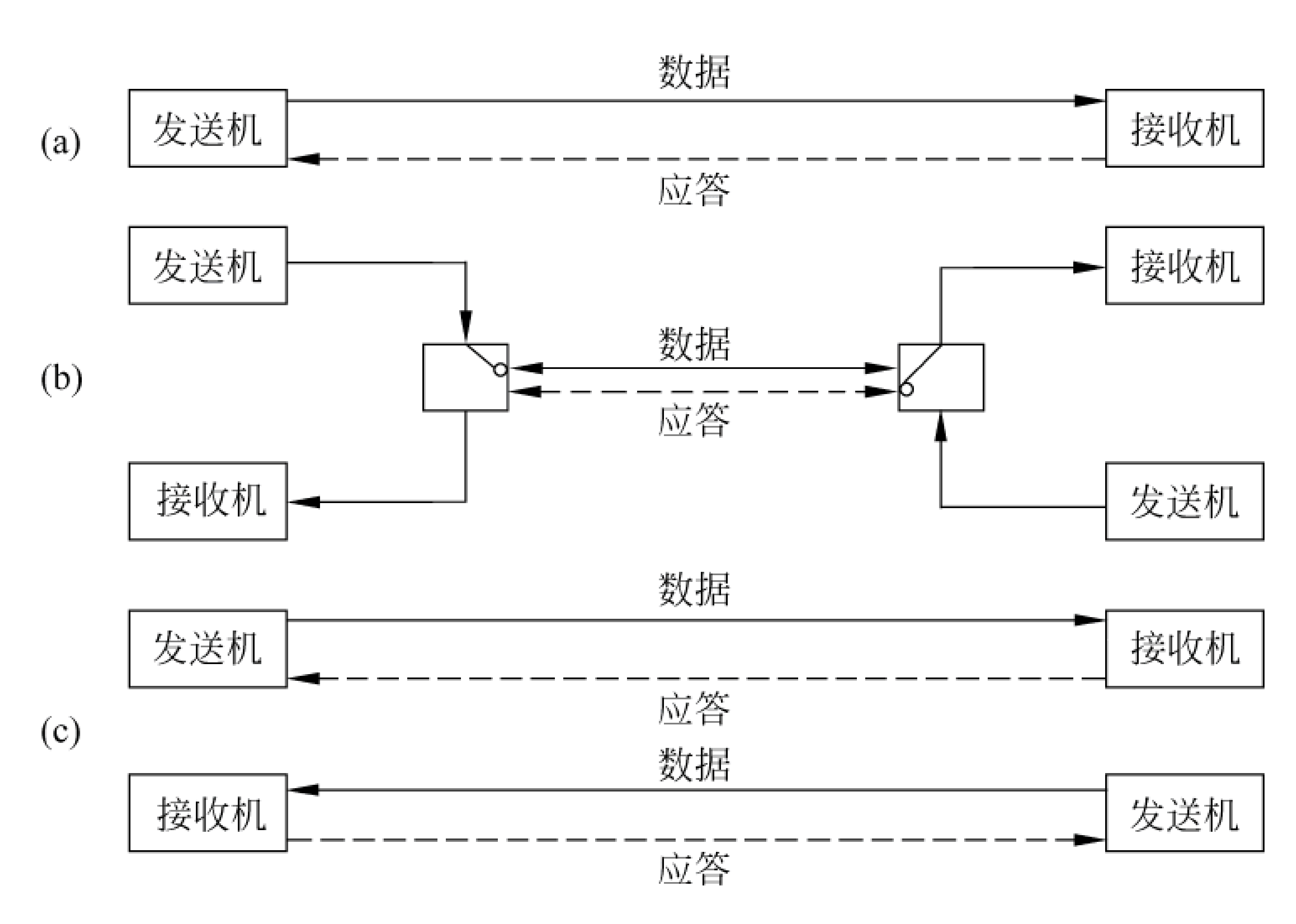


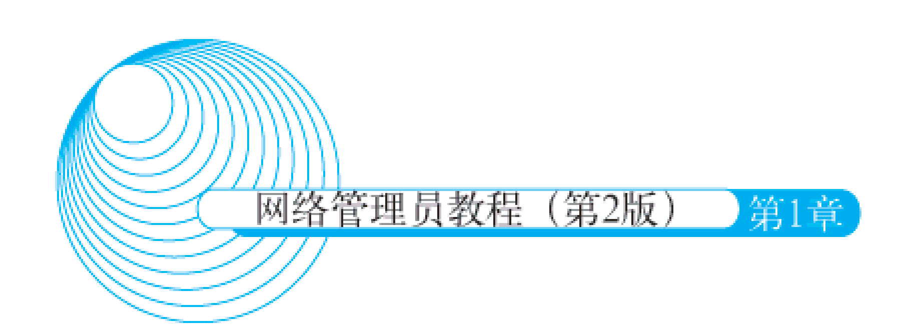
图 1-3 数据通信方式

1.1.2 数据传输

1. 数据传输的方式

1）并行传输与串行传输

并行传输指的是数据以成组的方式，在多条并行信道上同时进行传输。常用的就是将构成一个字符代码的几位二进制码，分别在几个并行信道上进行传输。例如，采用 8 单位代码的字符，可以用 8 个信道并行传输，一次传送一个字符，因此收、发双方不存在字符的同步问题，不需



要另加“起”、“止”信号或其他同步信号来实现收、发双方的字符同步，这是并行传输的一个主要优点。但是，并行传输必须有并行信道，这往往带来了设备上或实施条件上的限制，因此，实际应用受限。

串行传输指的是数据流以串行方式，在一条信道上传输。一个字符的 8 个二进制代码，由高位到低位顺序排列，再接下一个字符的 8 位二进制码，这样串接起来形成串行数据流传输。串行传输只需要一条传输信道，易于实现，是目前采用的一种主要传输方式。但是串行传输存在一个收、发双方如何保持码组或字符同步的问题，这个问题不解决，接收方就不能从接收到的数据流中正确地区分出一个个字符来，因而传输将失去意义。如何解决码组或字符的同步问题，目前有两种不同的解决办法，即异步传输方式和同步传输方式。

2）异步传输与同步传输

异步传输一般以字符为单位，不论所采用的字符代码长度为多少位，在发送每一字符代码时，前面均加上一个“起”信号，其长度规定为 1 个码元，极性为“0”，即空号的极性；字符代码后面均加上一个“止”信号，其长度为 1 或 2 个码元，极性皆为“1”，即与信号极性相同，加上起、止信号的作用就是为了能区分串行传输的“字符”，也就是实现了串行传输收、发双方码组或字符的同步。这种传输方式的优点是同步实现简单，收发双方的时钟信号不需要严格同步，缺点是对每一字符都需加入“起、止”码元，使传输效率降低，故适用于 1200bps 以下的低速数据传输。

同步传输是以同步的时钟节拍来发送数据信号的，因此在一个串行的数据流中，各信号码元之间的相对位置都是固定的（即同步的）。接收端为了从收到的数据流中正确地区分出一个个信号码元，首先必须建立准确的时钟信号。数据的发送一般以组（帧）为单位，是通过传输特定的传输控制字符或同步序列来完成的，传输效率较高。

2. 数据传输的形式

1）基带传输

在信道上直接传输基带信号，称为基带传输，它是指在通信电缆上原封不动地传输由计算机或终端产生的 0 或 1 数字脉冲信号。这样一个信号的基本频带可以从直流成分到数兆赫，频带越宽，传输线路的电容电感等对传输信号波形衰减的影响越大，传输距离一般不超过 2km，超过时则需加中继器放大信号，以便延长传输距离。基带信号绝大部分是数字信号，计算机网络内往往采用基带传输。

2）频带传输

将基带信号转换为频率表示的模拟信号来传输，称为频带传输。例如，使用电话线进行远距离数据通信，需要将数字信号调制成音频信号再发送和传输，接收端再将音频信号解调成数字信号。由此可见，采用频带传输时，要求在发送和接收端安装调制解调器，这不仅解决了数字信号可用电话线路传输，而且可以实现多路复用，从而提高了信道利用率。

3）宽带传输

将信道分成多个子信道，分别传送音频、视频和数字信号，称为宽带传输。它是一种传输介质的频带宽度较宽的信息传输，通常在300～400MHz左右。系统设计时将此频带分割成几个子频带，采用“多路复用”技术。一般来说，宽带传输与基带传输相比有以下优点：能在一个信道中传输声音、图像和数据信息，使系统具有多种用途；一条宽带信道能划分为多条逻辑基带信道，实现多路复用，因此信道的容量大大增加；宽带传输的距离比基带远，因为基带传输直接传送数字信号，传输的速率愈高，能够传输的距离愈短。

3. 数据传输速率

1）比特率

比特率指单位时间内所传送的二进制码元的有效位数，以每秒多少比特数计，即bps。例如一个数字通信系统，它每秒传输800个二进制码元，它的比特率是800比特/秒(bps)。码元是对于网络中传送的二进制数字中每一位的通称，也常称作“位”或bit。例如1010101，共有7位或7bit。

2）波特率

波特率是脉冲信号经过调制后的传输速率，它是指单位时间(秒)内传输的码元数目，以波特(Baud)为单位，通常用于表示调制器之间传输信号的速率。这里的码元可以是二进制的，也可以是多进制的。波特率N和比特率R的关系为$R=N\log_2 M$，当码元为二进制时，M为2；码元为四进制时，M为4，依此类推。如果波特率为600Baud，在二进制时，比特率为600bps，在八进制时为1800bps。

3）误码率

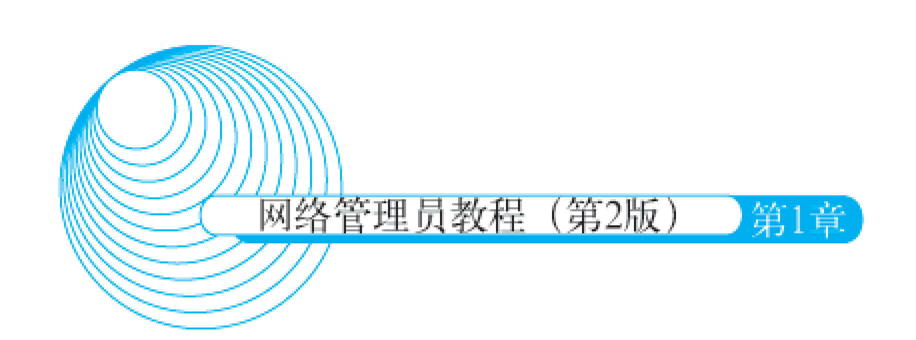
误码率指信息传输的错误率，是衡量系统可靠性的指标。它以接收信息中错误比特数占总传输比特数的比例来度量，通常应低于10^{-6}。

1.1.3 数据编码

在计算机中数据是以离散的二进制比特流方式表示的，称其为数字数据。计算机数据在网络中传输，通信信道无外乎两种类型，模拟信道和数字信道。计算机数据在不同的信道中传输要采用不同的编码方式，也就是说，在模拟信道中传输时，要把计算机中的数字信号，转换成模拟信道能够识别的模拟信号；在数字信道中传输时，要把计算机中的数字信号，转换成网络媒体能够识别的，利于网络传输的数字信号。

1. 模拟数据编码

将计算机中的数字数据在网络中用模拟信号表示，要进行调制，也就是要进行波形变换，或



者更严格地讲，是进行频谱变换，将数字信号的频谱变换成适合于在模拟信道中传输的频谱。最基本的调制方法有以下 3 种：

1）调幅（AM，Amplitude Modulation）

调幅即载波的振幅随着基带数字信号而变化，例如数字信号 1 用有载波输出表示，数字信号 0 用无载波输出表示，如图 1-4（a）所示。这种调幅的方法又叫幅移键控（ASK，Amplitude Shift Keying），其特点是信号容易实现，技术简单，但抗干扰能力差。

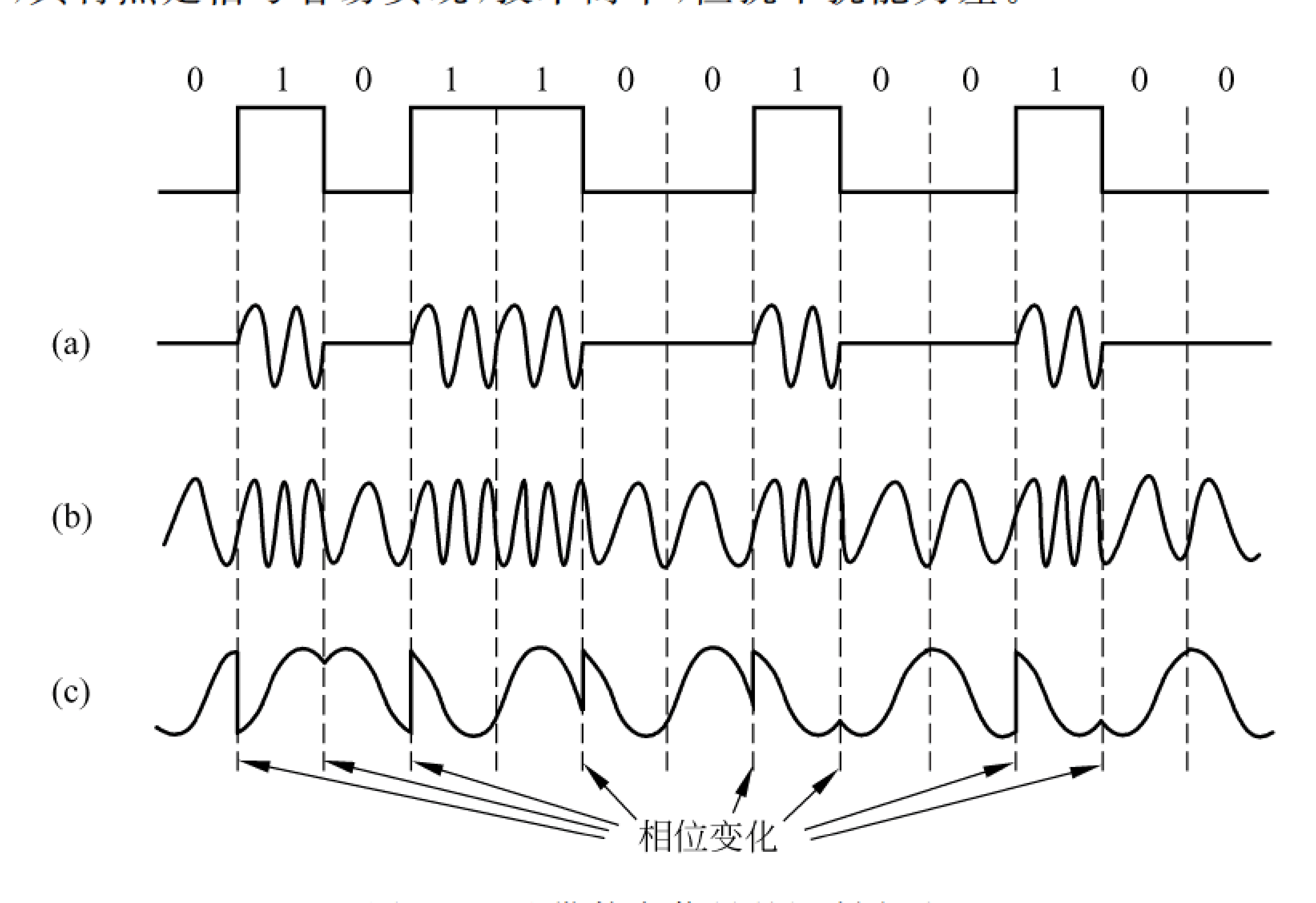


图 1-4　基带数字信号的调制方法

2）调频（FM，Frequency Modulation）

调频即载波的频率随着基带数字信号而变化，例如数字信号 1 用频率 f1 表示，数字信号 0 用频率 f2 表示，如图 1-4（b）所示。这种调频的方法又叫频移键控（FSK，Frequency Shift Keying），其特点是信号容易实现，技术简单，抗干扰能力较强。

3）调相（PM，Phase Modulation）

调相即载波的初始相位随着基带数字信号而变化，例如数字信号 1 对应于相位 180°，数字信号 0 对应于相位 0°，如图 1-4（c）所示。这种调相的方法又叫相移键控（PSK，Phase Shift Keying），其特点是抗干扰能力较强，但信号实现的技术比较复杂。

2. 数字数据编码

在数字信道中传输计算机数据时，要对计算机中的数字信号重新编码进行基带传输。在基带传输中，数字信号的编码方式主要有以下几种。

1）不归零编码 NRZ（Non-Return-Zero）

不归零编码用低电平表示二进制 0，用高电平表示二进制 1，如图 1-5(a)所示。

NRZ 码的缺点是无法判断每一位的开始与结束，收发双方不能保持同步。为保证收发双方同步，必须在发送 NRZ 码的同时，用另一个信道同时传送同步信号。

2）曼彻斯特编码(Manchester Encoding)

曼彻斯特编码不用电平的高低表示二进制，而是用电平的跳变来表示的。在曼彻斯特编码中，每一个比特的中间均有一个跳变，这个跳变既作为时钟信号，又作为数据信号。电平从高到低的跳变表示二进制 0，从低到高的跳变表示二进制 1，如图 1-5(b)所示。

3）差分曼彻斯特编码(Differential Manchester Encoding)

差分曼彻斯特编码是对曼彻斯特编码的改进，每比特中间的跳变仅做同步之用，每比特的值根据其开始边界是否发生跳变来决定。每比特的开始无跳变表示二进制 1，有跳变表示二进制 0，如图 1-5(c)所示。

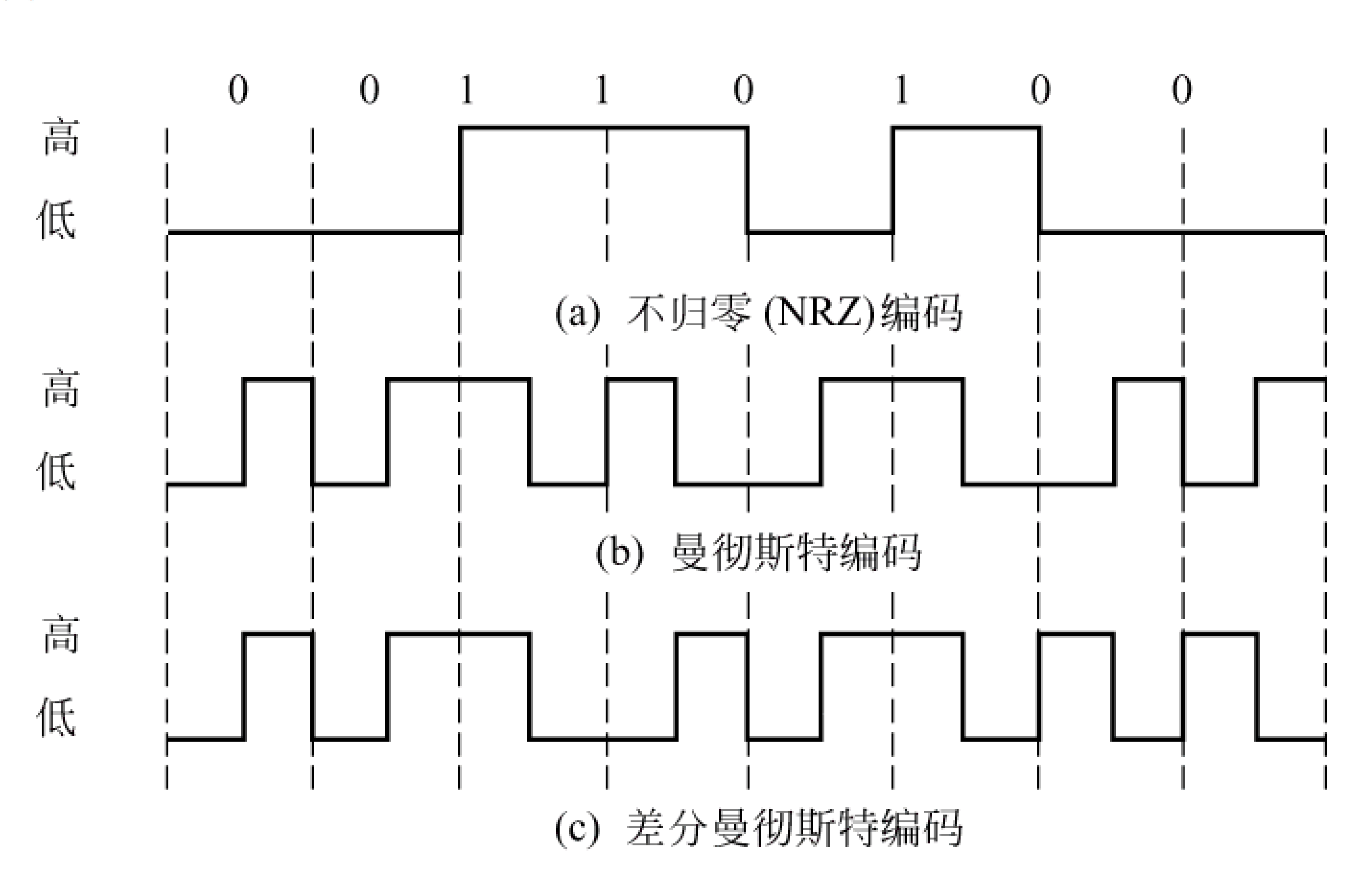
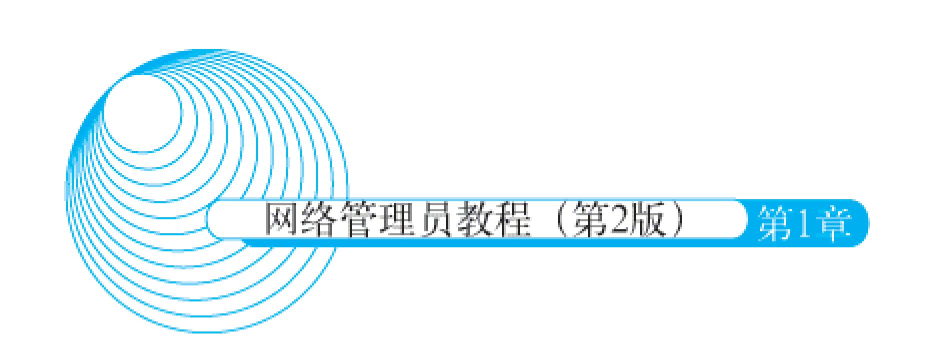


图 1-5　数字信号的编码

曼彻斯特编码和差分曼彻斯特编码是数据通信中最常用的数字信号编码方式，它们的优点是明显的，那就是无须另发同步信号。但缺点也是明显的，那就是编码效率低，如果传送 10Mbps 的数据，那么需要 20MHz 的脉冲。

1.1.4　多路复用技术

为了充分利用传输媒体，人们研究了在一条物理线路上建立多个通信信道的技术，这就是多路复用技术。多路复用技术的实质是，将一个区域的多个用户数据通过发送多路复用器进行汇集，然后将汇集后的数据通过一条物理线路进行传送，接收多路复用器再对数据进行分离，分发到多个用户。多路复用通常分为频分多路复用、时分多路复用、波分多路复用、码分多址和空分多址。



1. 频分多路复用（FDM，Frequency Division Multiplexing）

事实上，通信线路的可用带宽超过了给定信号的带宽。频分多路复用恰恰是利用了这一优点。频分多路复用的基本原理是：如果每路信号以不同的载波频率进行调制，而且各个载波频率是完全独立的，即各个信道所占用的频带不相互重叠。相邻信道之间用“警戒频带”隔离，那么每个信道就能独立地传输一路信号。其基本原理如图 1-6 所示。

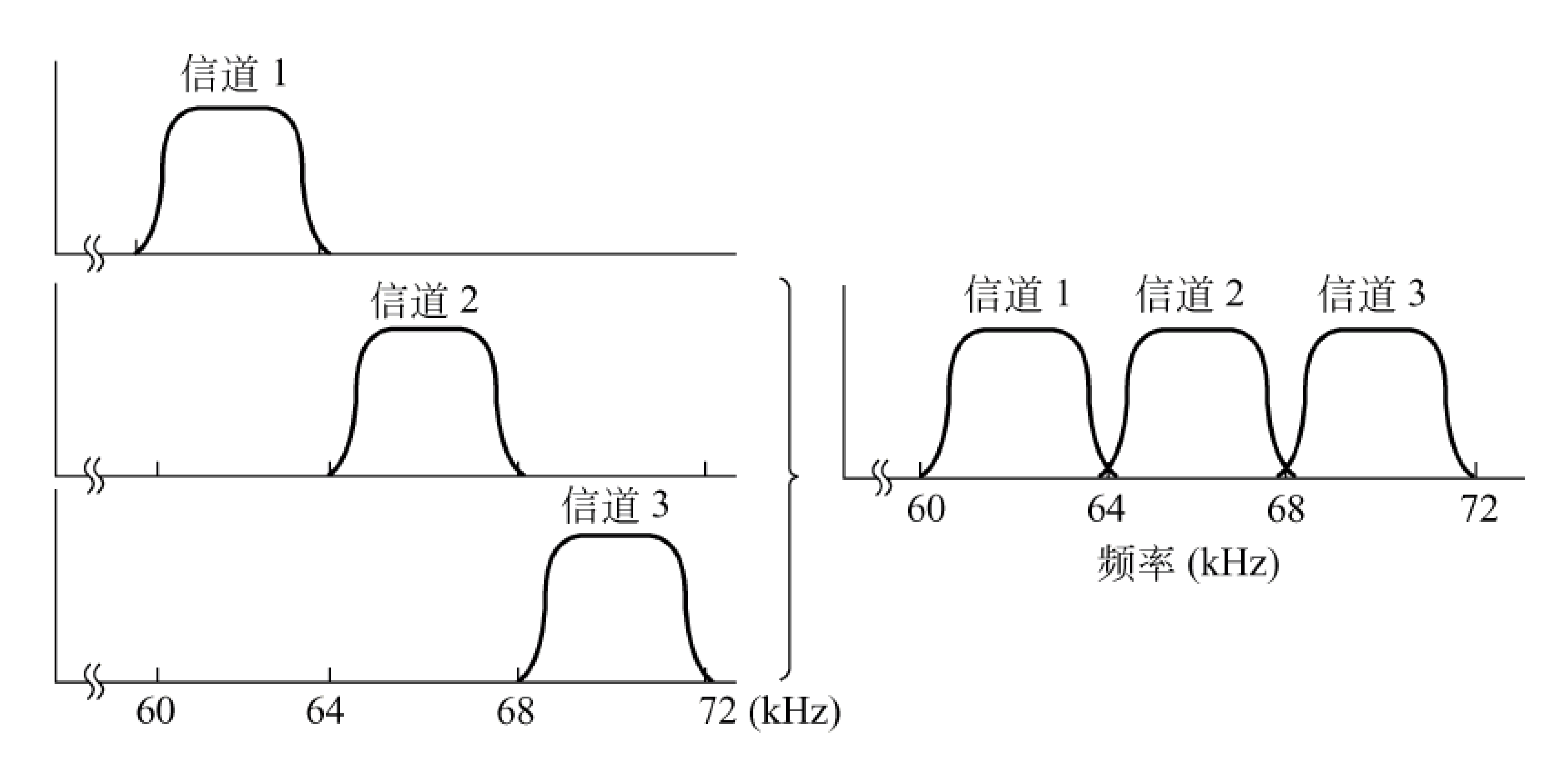


图 1-6　频分多路复用

频分多路复用的主要特点是，信号被划分成若干通道（频道，波段），每个通道互不重叠，独立进行数据传递。频分多路复用在无线电广播和电视领域中应用较多。ADSL 也是一个典型的频分多路复用。ADSL 用频分多路复用的方法，在 PSTN 使用的双绞线上划分出 3 个频段：0～4kHz 用来传送传统的语音信号；20～50kHz 用来传送计算机上载的数据信息；150～500kHz 或 140～1100kHz 用来传送从服务器上下载的数据信息。

2. 时分多路复用（TDM，Time Division Multiplexing）

时分多路复用是以信道传输时间作为分割对象，通过为多个信道分配互不重叠的时间片的方法来实现多路复用。时分多路复用将用于传输的时间划分为若干个时间片，每个用户分得一个时间片。

时分多路复用通信，是各路信号在同一信道上占有不同时间片进行通信。由抽样理论可知，抽样的一个重要作用，是将时间上连续的信号变成时间上离散的信号，其在信道上占用时间的有限性，为多路信号沿同一信道传输提供了条件。具体说，就是把时间分成一些均匀的时间片，将各路信号的传输时间分配在不同的时间片，以达到互相分开，互不干扰的目的。图 1-7 为时分多路复用示意图。

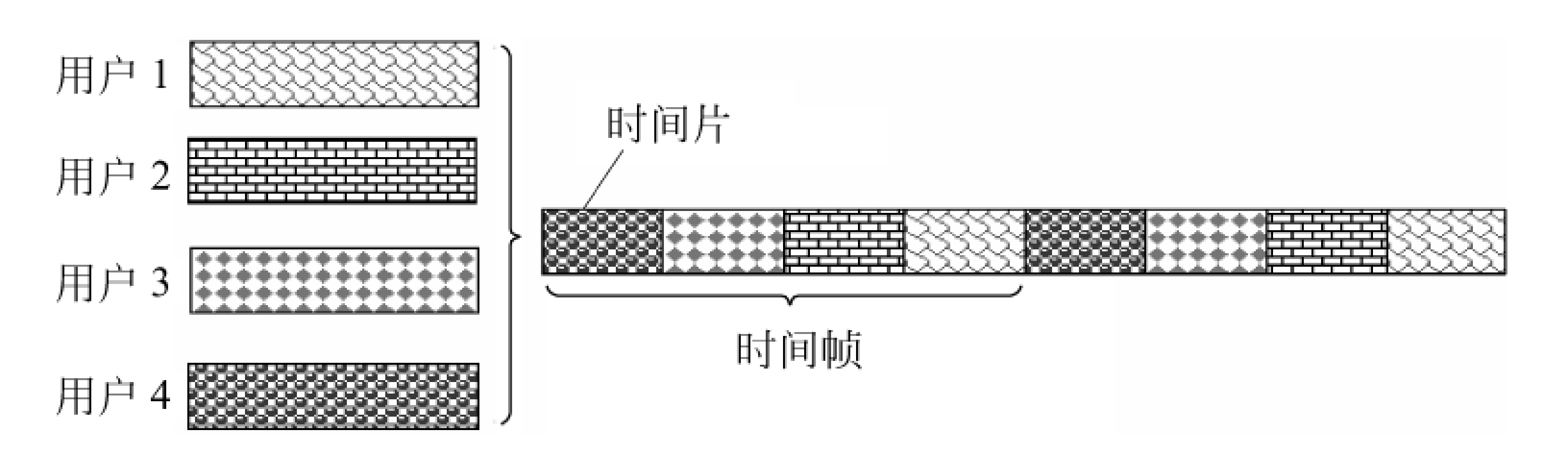


图 1-7 时分多路复用

目前，应用最广泛的时分多路复用是贝尔系统的 T1 载波。T1 载波是将 24 路音频信道复用在一条通信线路上，每路音频信号在送到多路复用器之前，要通过一个脉冲编码调制（PCM，Pulse Code Modulation）编码器，编码器每秒取样 8000 次。24 路信号的每一路，轮流将一个字节插入到帧中，每个字节的长度为 8bit，其中 7bit 是数据位，1bit 用于信道控制。每帧由 24×8=192bit 组成，附加 1bit 作为帧的开始标志位，所以每帧共有 193bit。由于发送一帧需要 125μs，一秒钟可以发送 8000 帧。因此 T1 载波的数据传输速率为：

193bit×8000/s=1544000bps=1544kbps=1.544Mbps

3. 波分多路复用（WDM，Wavelength Division Multiplexing）

什么叫波分复用？所谓波分复用就是在同一根光纤内传输多路不同波长的光信号，以提高单根光纤的传输能力。因为目前光通信的光源在光通信的“窗口”上只占用了很窄的一部分，还有很大的范围没有利用。也可以这样认为：WDM 是 FDM 应用于光纤信道的一个变例。如果让不同波长的光信号在同一根光纤上传输而互不干扰，利用多个波长适当错开的光源同时在一根光纤上传送各自携带的信息，就可以大大增加所传输的信息容量。由于是用不同的波长传送各自的信息，因此即使在同一根光纤上也不会相互干扰。在接收端转换成电信号时，可以独立地保持每一个不同波长的光源所传送的信息。这种方式就叫做“波分复用”。其基本原理如图 1-8 所示。

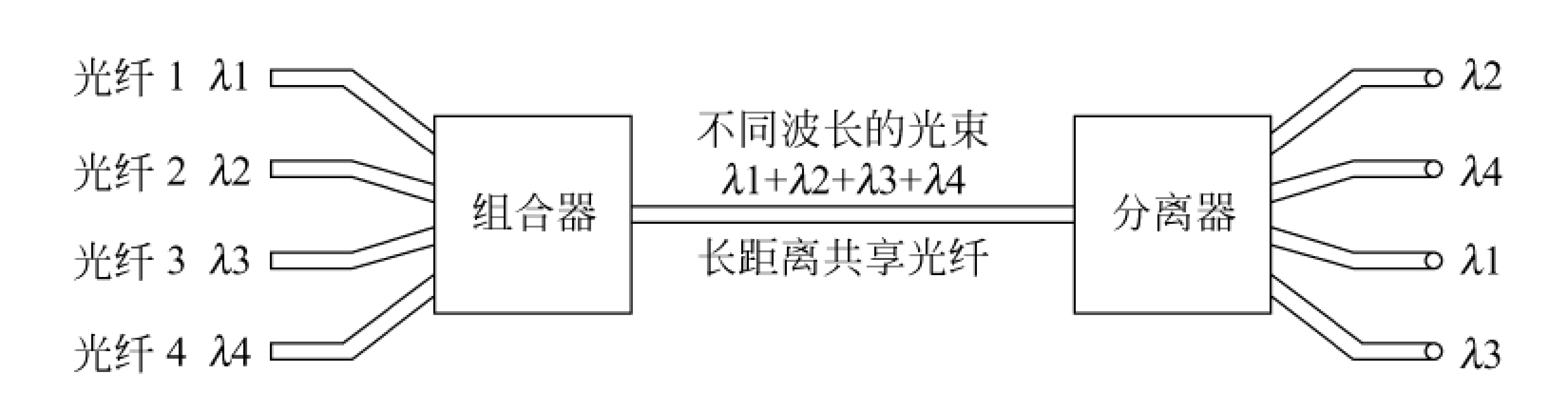
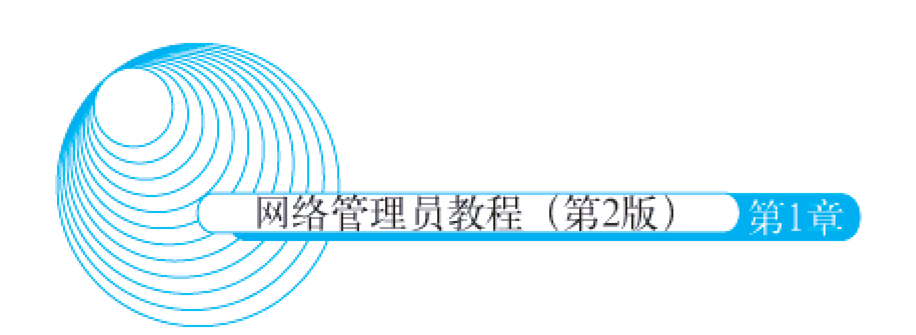


图 1-8 波分多路复用

如果将一系列载有信息的不同波长的光载波，在光频域内以一至几百纳米的波长间隔合在



一起沿单根光纤传输，在接收端再用一定的方法，将各个不同波长的光载波分开，在光纤的工作窗口上安排100个波长不同的光源，同时在一根光纤上传送各自携带的信息，就能使光纤通信系统的容量提高100倍。

4. 码分多址(CDMA，Code Division Multiple Access)

CDMA又称为码分多址，采用地址码和时间、频率共同区分信道的方式。CDMA的特征是每个用户具有特定的地址码，而地址码之间相互具有正交性，因此各用户信息的发射信号在频率、时间和空间上都可能重叠，从而使有限的频率资源得到利用。

CDMA是在扩频技术上发展起来的无线通信技术，即将需要传送的具有一定信号带宽的信息数据，用一个带宽远大于信号带宽的高速伪随机码进行调制，使原数据信号的带宽被扩展，再经载波调制并发送出去。接收端也使用完全相同的伪随机码，对接收的带宽信号作相关处理，把宽带信号换成原信息数据的窄带信号即解扩，以实现信息通信。不同的移动台(或手机)可以使用同一个频率，但是每个移动台(或手机)都被分配带有一个独特的“码序列”，该序列码与所有别的“码序列”都不相同，因为是靠不同的“码序列”来区分不同的移动台(或手机)，所以各个用户相互之间也没有干扰，从而达到了多路复用的目的。

5. 空分多址(SDMA，Space Division Multiple Access)

空分多址(SDMA)：这种技术是将空间分割构成不同的信道，从而实现频率的重复使用，达到信道增容的目的。举例来说，在一颗卫星上使用多个天线，各个天线的波束射向地球表面的不同区域，地面上不同地区的地球站，在同一时间，即使使用相同的频率进行工作，它们之间也不会形成干扰。SDMA系统的处理程序如下：

(1) 系统将首先对来自所有天线中的信号进行快照或取样，然后将其转换成数字形式，并存储在内存中。

(2) 计算机中的SDMA处理器将立即分析样本，对无线环境进行评估，确认用户、干扰源及其所在的位置。

(3) 处理器对天线信号的组合方式进行计算，力争最佳地恢复用户的信号。借助这种策略，每位用户的信号接收质量将大大提高，而其他用户的信号或干扰信号则会遭到屏蔽。

(4) 系统将进行模拟计算，使天线阵列可以有选择地向空间发送信号。在此基础上，每位用户的信号都可以通过单独的通信信道——空间信道实现高效的传输。

(5) 在上述处理的基础上，系统就能够在每条空间信道上发送和接收信号，从而使这些信道成为双向信道。

利用上述流程，SDMA系统就能够在一条普通信道上创建大量的频分、时分或码分双向空间信道，每一条信道都可以完全获得整个阵列的增益和抗干扰功能。从理论上而言，带有 m 个

单元的阵列能够在每条普通信道上支持 m 条空间信道。但在实际应用中支持的信道数量将略低于这个数目，具体情况则取决于环境。由此可见，SDMA 系统可使系统容量成倍增加，使得系统在有限的频谱内可以支持更多的用户，从而成倍地提高频谱使用效率。

近几十年来，无线通信经历了从模拟到数字，从固定到移动的重大变革。而就移动通信而言，为了更有效地利用有限的无线频率资源，时分多址技术（TDMA）、频分多址技术（FDMA）、码分多址技术（CDMA）得到了广泛的应用，并在此基础上建立了 GSM 和 CDMA（是区别于 3G 的窄带 CDMA）两大主要的移动通信网络。就技术而言，现有的这 3 种多址技术已经得到了充分的应用，频谱的使用效率已经发挥到了极限。空分多址技术（SDMA）则突破了传统的三维思维模式，在传统的三维技术的基础上，在第四维空间上极大地拓宽了频谱的使用方式，使得移动用户仅仅由于空间位置的不同而复用同一个传统的物理信道成为可能，并将移动通信技术引入了一个更为崭新的领域。

1.1.5 数据交换技术

1. 电路交换

在数据通信网发展初期，人们根据电话交换原理，发展了电路交换方式。当用户要发信息时，由源交换机根据信息要到达的目的地址，把线路接到那个目的交换机。这个过程称为线路接续，是由所谓的联络信号经存储转发方式完成的，即根据用户号码或地址（被叫），经局间中继线传送给被叫交换局并转被叫用户。线路接通后，就形成了一条端对端（用户终端和被叫用户终端之间）的信息通路，在这条通路上双方即可进行通信。通信完毕，由通信双方的某一方，向自己所属的交换机发出拆除线路的要求，交换机收到此信号后就将此线路拆除，以供别的用户呼叫使用。电路交换与电话交换方式的工作过程很类似，如图 1-9 所示。

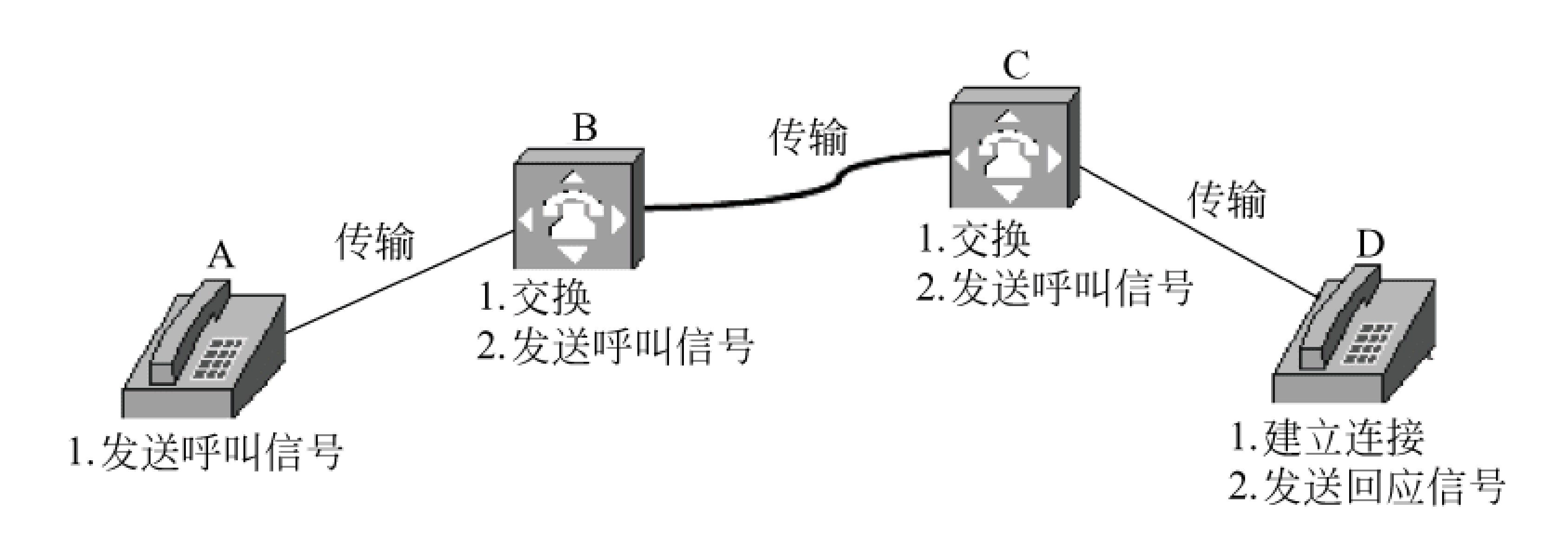
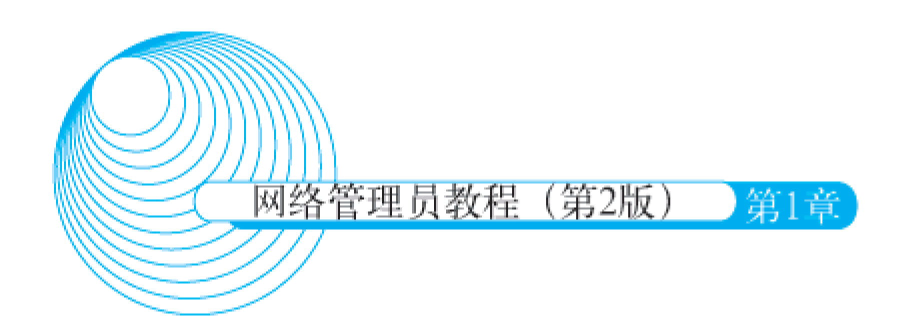


图 1-9 电路交换示意

主机 A 要向主机 D 传送数据，首先要通过通信子网 B 和 C 在 A 和 D 之间建立连接。首先主机 A 向节点 B 发送呼叫信号，其中含有要建立连接的主机 D 的目的地址；节点 B 根据目的地址和路径选择算法，选择下一个节点 C，并向节点 C 发送呼叫信号；节点 C 根据目的地址和路径



选择算法，选择目的主机 D，并向主机 D 发送呼叫信号；主机 D 如果接收呼叫请求，它一方面建立连接，一方面通过已建立的连接 A—B—C—D，向主机 A 发送呼叫回应包。

由于电路交换的接续路径是采用物理连接的，在传输电路接续后，控制电路就与信息传输无关，所以电路交换方式的主要优点是：数据传输可靠、迅速，不丢失且保持原来的序列。缺点是在有的环境下，电路空闲时的信道容量被浪费，而且数据传输阶段的持续时间不长的话，电路建立和拆除所用的时间也得不偿失。因此它适合于系统间要求高质量的大量数据传输的情况，其计费方法一般按照预定的带宽、距离和时间来计算。

2. 报文交换

20 世纪 60 年代和 70 年代，为了获得较好的信道利用率，出现了存储-转发的想法，这种交换方式就是报文交换。目前这种技术仍普遍应用在某些领域(如电子信箱等)。

在报文交换中，不需要在两个站之间建立一条专用通路，其数据传输的单位是报文，即站点一次性要发送的数据块，长度不限且可变。传送的方式采用存储-转发方式，即一个站想要发送一个报文，它把一个目的地址附加在报文上，网络节点根据报文上的目的地址信息，把报文发送到下一个节点，一直逐个节点地转送到目的节点。每个节点在收下整个报文之后，检查无错误后，暂存这个报文，然后利用路由信息找出下一个节点的地址，再把整个报文传送给下一个节点，因此，端与端之间无须先通过呼叫建立连接。

它的基本原理是用户之间进行数据传输，主叫用户不需要先建立呼叫，而先进入本地交换机存储器，等到连接该交换机的中继线空闲时，再根据确定的路由转发到目的交换机。由于每份报文的头部都含有被寻址用户的完整地址，所以每条路由不是固定分配给某一个用户，而是由多个用户进行统计复用。

报文交换与邮信件的工作过程很类似，信(报文)邮出去时，写好目的地址，就交给邮局(通信子网)了，至于信如何分发，走哪条路，信源节点都不管，完全交给邮局处理，如图 1-10 所示。

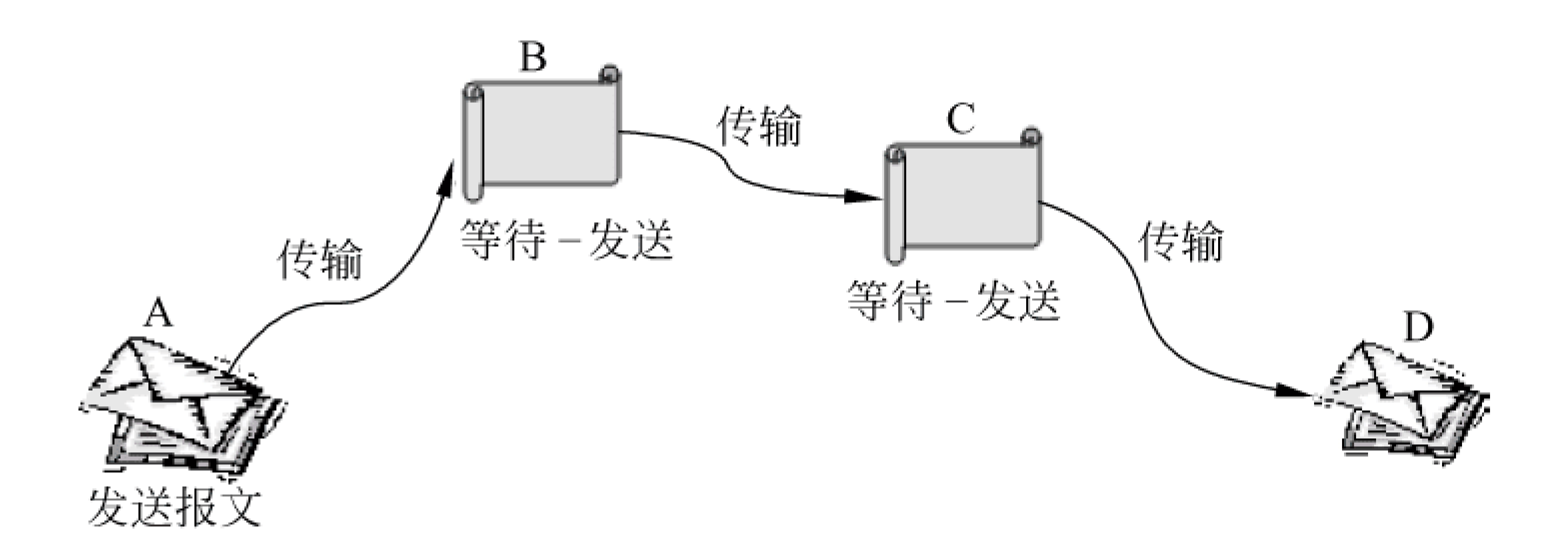


图 1-10　报文交换示意

这种方法比起电路交换来有许多优点：

(1) 线路效率较高。这是因为许多报文可以分时共享一条节点的通道。对于同样的通信容量来说，需要较小的传输能力。

(2) 不需要同时使用发送器和接收器来传输数据，网络可以在接收器可用之前，暂时存储这个报文。

(3) 在电路交换网络上，当通信量变得很大时，就不能接受某些呼叫，而在报文交换网络上，却仍然可以接收报文，但传送延迟会增加。

(4) 报文交换系统可以把一个报文发送到多个目的地，而电路交换网络很难做到这一点。

报文交换的主要缺点是，它不能满足实时或交互式的通信要求，经过网络的延迟相当长，而且有相当大的变化。因此，这种方式不能用于声音连接，也不适合于交互式终端到计算机的连接。有时节点收到过多的数据而不得不丢弃报文，并阻止了其他报文的传送，而且发出的报文不按顺序到达目的地。另外，报文交换中，若报文较长，需要较大容量的存储器，若将报文放到外存储器中去时，会造成响应时间过长，增加了网络延迟时间。

3. 分组交换

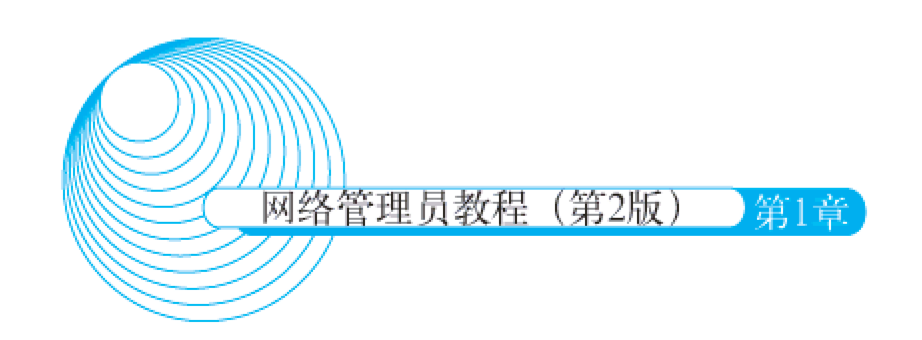
分组交换也称包交换，它是将用户传送的数据划分成一定的长度，每个部分叫做一个分组。分组交换与报文交换都是采用存储-转发交换方式。二者的主要区别是：报文交换时报文的长度不限且可变，而分组交换的报文长度不变。分组交换首先把来自用户的数据暂存于存储装置中，并划分为多个一定长度的分组，每个分组前边都加上固定格式的分组标题，用于指明该分组的发端地址、收端地址及分组序号等。

以报文分组作为存储转发的单位，分组在各交换节点之间传送比较灵活，交换节点不必等待整个报文的其他分组到齐，一个分组、一个分组地转发。这样可以大大压缩节点所需的存储容量，也缩短了网络时延。另外，较短的报文分组比长的报文可大大减少差错的产生，提高了传输的可靠性。

分组交换通常有两种方式：数据包方式和虚电路方式。数据包方式，是每一个数据分组都包含终点地址信息，分组交换机为每一个数据分组独立地寻找路径。因一份报文包含的不同分组，可能沿着不同的路径到达终点，在网络终点需要重新排序。在分组交换网中还有另外一种方式，叫做虚电路方式。所谓虚电路，就是两个用户终端设备在开始互相发送和接收数据之前，需要通过网路建立逻辑上的连接，一旦这种连接建立之后，就在网路中保持已建立的数据通路，用户发送的数据(以分组为单位)将按顺序通过网络到达终点。当用户不需要发送和接收数据时，可以清除这种连接。

在分组交换方式中，由于能够以分组方式进行数据的暂存交换，经交换机处理后，很容易地实现不同速率、不同规程的终端间通信。分组交换的特点主要有：

(1) 线路利用率高。分组交换以虚电路的形式进行信道的多路复用，实现资源共享，可在一



条物理线路上提供多条逻辑信道，极大地提高了线路的利用率。

（2）不同种类的终端可以相互通信。数据以分组为单位在网络内存储转发，使不同速率终端、不同协议的设备经网络提供的协议变换功能后实现互相通信。

（3）信息传输可靠性高。每个分组在网络中进行传输时，在节点交换机之间采用差错校验与重发的功能，因而在网络中传送的误码率大大降低。而且当网络内发生故障时，网络中的路由机制会使分组自动地选择一条新的路由以避开故障点，不会造成通信中断。

（4）分组多路通信。由于每个分组都包含有控制信息，所以分组型终端可以同时与多个用户终端进行通信，可把同一信息发送到不同用户。

4. 信元交换

普通的电路交换和分组交换都很难胜任宽带高速交换的交换任务。对于电路交换，当数据的传输速率及其变化非常大时，交换的控制就变得十分复杂；对于分组交换，当数据传输速率很高时，协议数据单元在各层的处理就成为很大的开销，无法满足实时性要求很强的业务需求。但电路交换的实时性很好，分组交换的灵活性很好。于是，一种结合这两种交换方式优点的交换技术——信元交换产生了。

信元交换又叫异步传输模式（ATM，Asynchronous Transfer Mode），是一种面向连接的快速分组交换技术，它是通过建立虚电路来进行数据传输的。ATM 采用固定长度的信元作为数据传送的基本单位，信元长度为 53 字节，其中信元头为 5 字节，数据为 48 字节。长度固定的信元可以使 ATM 交换机的功能尽量简化，只用硬件电路就可以对信元头中的虚电路标识进行识别，因此大大缩短了每一个信元的处理时间。另外 ATM 采用了统计时分复用的方式来进行数据传输，根据各种业务的统计特性，在保证服务质量要求（QoS，Quality of Service）的前提下，在各个业务之间动态地分配网络带宽。

1.2　计算机网络简介

1.2.1　计算机网络的概念

计算机从诞生到现在已经有 50 多年的历史了。随着时代的发展，面对浩如烟海的信息与知识，仅仅依靠单个计算机“孤军奋战”已经难以发挥更大作用了。于是，人们开始注意到计算机网络的使用。

计算机网络是现代通信技术与计算机技术相结合的产物。所谓计算机网络，就是把分布在不同地理区域的计算机与专用外部设备用通信线路互联成一个规模大、功能强的计算机应用系统，从而使众多的计算机可以方便地互相传递信息，共享硬件、软件、数据信息等资源。人们组建计算机网络的目的是为了实现计算机之间的资源共享，因此，网络提供资源的多少决定了一

个网络的存在价值。计算机网络的规模有大有小，大的可以覆盖全球，小的可以仅由一间办公室中的两台或几台计算机构成。通常，网络规模越大，包含计算机越多，它所提供的网络资源就越丰富，其价值也就越高。

从定义中看出计算机网络涉及3个方面的问题：

（1）至少有两台计算机互联。

（2）通信设备与线路介质。

（3）网络软件，是指通信协议和网络操作系统。

计算机网络的应用正在改变着人们的工作与生活方式，正在进一步引起世界范围内产业结构的变化，促进全球信息产业的发展。人们已经看到：计算机越普及、应用范围越广，就越需要互联起来构成网络。在信息技术高速发展的今天，“计算机就是网络，网络就是计算机”的概念越来越被人们所接受，计算机应用正在进入一个全新的网络时代。

1.2.2 计算机网络的分类

计算机网络的种类很多，通常是按照规模大小和延伸范围来分类的，根据不同的分类原则，可以得到不同类型的计算机网络。按网络覆盖的范围大小不同，计算机网络可分为局域网（LAN，Local Area Network）、城域网（MAN，Metropolitan Area Network）、广域网（WAN，Wide Area Network）；按照网络的拓扑结构来划分，计算机网络可以分为环型网、星型网、总线型网等；按照通信传输介质来划分，可以分为双绞线网、同轴电缆网、光纤网、微波网、卫星网、红外线网等；按照信号频带占用方式来划分，又可以分为基带网和宽带网。

（1）局域网：是指在较小的地理范围内（一般小于10km）由计算机、通信线路（一般为双绞线）和网络连接设备（一般为集线器和交换机）组成的网络。

（2）城域网：是指在一个城市范围内（一般小于100km）由计算机、通信线路（包括有线介质和无线介质）和网络连接设备（一般为集线器、交换机和路由器等）组成的网络。

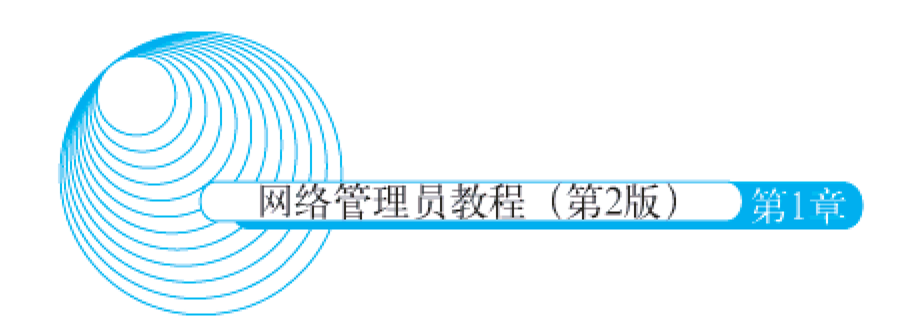
（3）广域网：比城域网范围大，由多个局域网或城域网组成的网络。目前，已不能明确区分广域网和城域网，或者也可以说城域网的概念越来越模糊了，因为在实际应用中，已经很少有封闭在一个城市内的独立网络。因特网（Internet）是世界上最大的广域网。

1.2.3 计算机网络的构成

和计算机系统一样，一个完整的计算机网络系统也是由硬件系统和软件系统两大部分组成的。

1. 网络硬件

网络硬件一般是指计算机设备、传输介质和网络连接设备。目前，网络连接设备有很多，功



能不一，也很复杂。

网络中的计算机，根据其作用不同，可分为服务器和工作站。服务器的主要功能是通过网络操作系统控制和协调网络各工作站的运行，处理和响应各工作站同时发来的各种网络操作要求，提供网络服务。工作站是网络各用户的工作场所，通常是一台微机或终端。工作站通过插在其中的网络接口板（网卡）经传输介质与网络服务器相连。

按照提供的应用类型网络服务器可分为：文件服务器、应用程序服务器、通信服务器几大类。通常一个网络至少有一个文件服务器，网络操作系统及其实用程序和共享硬件资源都安装在文件服务器上。文件服务器只为网络提供硬盘共享、文件共享、打印机共享等功能，工作站需要共享数据时，便从文件服务器中取过来，文件服务器只负责共享信息的管理、接收和发送，而丝毫不帮助工作站对所要求的信息进行处理。随着分布式网络操作系统和分布式数据库管理系统的出现，要求网络服务器不仅要具有文件服务器功能，而且要能够处理用户提交的任务。简单地说就是当某一网络工作站要对共享数据进行操作时，具体控制该操作的不仅是工作站上的处理器，还应有网络服务器上的处理器，即网络中有多个处理器为一个事务进行处理，具有这种能执行用户应用程序功能的服务器叫应用程序服务器。人们所说的一般微机局域网中的工作站并不共享网络服务器的 CPU 资源，如果有了应用程序服务器就可以实现了。若应用程序是一个数据库管理系统，则有时也称之为数据库服务器。

按照网络服务器的设计思想分类，一般把服务器分成 3 种类型：一种是入门级服务器，有时也称为 PC 服务器；一种是工作组级服务器，在中小企业的业务部门里使用，有时也称为部门级或工作组级服务器；还一种就是企业级服务器，一般担当企业的整体网络部署。

在目前的应用领域，入门级服务器产品较多，服务器处理器芯片主要有 Intel 公司的赛扬、奔腾和至强（Xeon）等，性能相差也不小，最常见的产品形态是采用了塔式服务器，有部分的产品是机架式，但是还比较少。部门级服务器主要适合 10～50 台电脑的网络环境，为了满足企业对数据和实时性的要求，部门级服务器大都拥有双处理器的服务器主板，低端部门级产品一般配备单个处理器，但是大半是至强芯片，除了胜任入门级服务器所有任务外，也为以后的升级预留了空间。中高端的就是双处理器了，通常也称它们为工作组级服务器。企业级服务器也同样采用 Intel 公司最新的 Xeon MP 处理器，另外通常采用可高达 8GB 的高速 PC1600 双倍数据速率（DDR）内存，它具有紧凑的 3U 机柜优化设计，集成 4 路计算功能，存储系统采用 SCSI 控制器，硬盘阵列驱动器容量可达千 GB 级，支持热拔插，在廉价磁盘冗余阵列（RAID，Redundant Array of Inexpensive Disks）技术的支持下，通过镜像或者存储奇偶校验信息的方式，实现对数据的冗余保护。

2．网络软件

网络软件一般是指系统级的网络操作系统、网络通信协议和应用级的提供网络服务功能的

专用软件。

1）网络操作系统

网络操作系统是用于管理网络的软、硬件资源，提供简单网络管理的系统软件。常见的网络操作系统有 UNIX、NetWare、Windows NT、Linux 等。UNIX 是一种强大的分时操作系统，以前在大型机和小型机上使用，现已向 PC 机过渡。UNIX 支持 TCP/IP 协议，安全性、可靠性强，缺点是操作使用复杂。常见的 UNIX 操作系统有 SUN 公司的 Solaris、IBM 公司的 AIX、HP 公司的 HP UNIX 等。NetWare 是 Novell 公司开发的早期局域网操作系统，使用 IPX/SPX 协议，目前的最新版本 NetWare 5.0 也支持 TCP/IP 协议，安全性、可靠性较强，其优点是具有 NDS 目录服务，缺点是操作使用较复杂。Windows NT Server 是 Microsoft 公司为解决 PC 机做服务器而设计的，操作简单方便，缺点是安全性、可靠性较差，适用于中小型网络。Linux 是一个免费的网络操作系统，源代码完全开放，是 UNIX 的一个分支，内核基本和 UNIX 一样，具有 Windows NT 的界面，操作较简单，缺点是应用程序较少。

2）网络通信协议

网络通信协议是网络中计算机交换信息时的约定，它规定了计算机在网络中互通信息的规则。因特网采用的协议是 TCP/IP，该协议也是目前应用最广泛的协议，其他常见的协议还有 Novell 公司的 IPX/SPX 等。

1.3 计算机网络硬件

1.3.1 计算机网络传输媒体

网络上数据的传输需要有“传输媒体”，这好比是车辆必须在公路上行驶一样，道路质量的好坏会影响到行车的安全舒适。同样，网络传输媒介的质量好坏也会影响数据传输的质量，包括速率、数据丢失等。

常用的网络传输媒介可分为两类：一类是有线的；一类是无线的。有线传输媒介主要有同轴电缆、双绞线及光缆；无线传输媒介主要有微波、无线电、激光和红外线等。

1. 同轴电缆(Coaxial Cable)

同轴电缆绝缘效果佳，频带较宽，数据传输稳定，价格适中，性价比高。同轴电缆中央是一根内导体铜质芯线，外面依次包有绝缘层、网状编织的外导体屏蔽层和塑料保护外层，如图 1-11 所示。

通常按特性阻抗数值的不同，可将同轴电缆分为 50Ω 基带同轴电缆和 75Ω 宽带同轴电缆。前者用于传输基带数字信号，是早期局域网的主要传输媒体；后者是有线电视系统 CATV 中的标准传输电缆，在这种电缆上传输的信号采用了频分复用的宽带模拟信号。

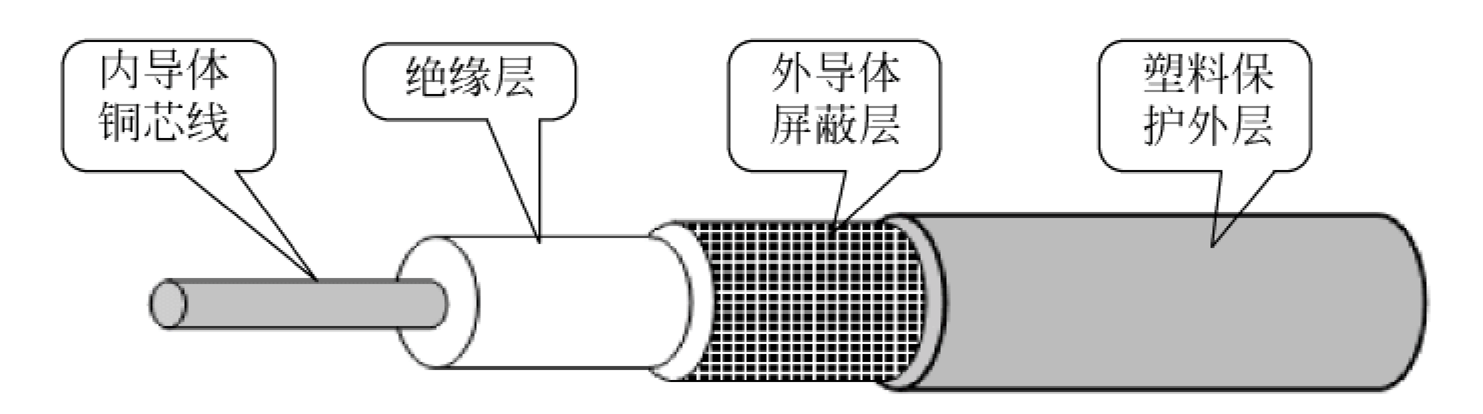


图 1-11　同轴电缆结构

50Ω 基带同轴电缆可分为两类：粗缆和细缆。粗缆用于 10Base5 以太网，最大干线长度 500m，最大网络干线电缆长度 2500m，每条干线段支持的最大节点数 100 个，收发器之间的最小距离 1.5m，收发器电缆的最大长度 50m；细缆用于 10Base2 以太网，最大干线段长度 185m，最大网络干线电缆长度 925m，每条干线段支持的最大节点数 30 个，BNC、T 型连接器之间的最小距离 0.5m。

使用基带同轴电缆组网，需要在两端连接 50Ω 的反射电阻，又叫终端匹配器。同轴电缆组网的其他连接设备，粗缆与细缆的不尽相同。在与粗缆连接时，收发器是外置在电缆上的，要使用 9 芯 D 型 AUI 接口，网卡上必须带有粗缆连接接口（通常在网卡上标有“DIX”）；在与细缆连接时，收发器是内置在网卡上的，需要 BNC 接口、T 型接口配合使用，网卡上必须带有细缆连接接口（通常在网卡上标有“BNC”）。

2. 双绞线（Twisted Pair）

双绞线是由两条导线按一定扭矩相互绞合在一起的类似于电话线的传输媒体，每根线加绝缘层并用颜色来标记，如图 1-12 的左部分所示。成对线的扭绞旨在使电磁辐射和外部电磁干扰减到最小。使用双绞线组网，双绞线与网卡、双绞线与集线器的接口叫 RJ45，俗称水晶头，如图 1-12 的右部分所示。

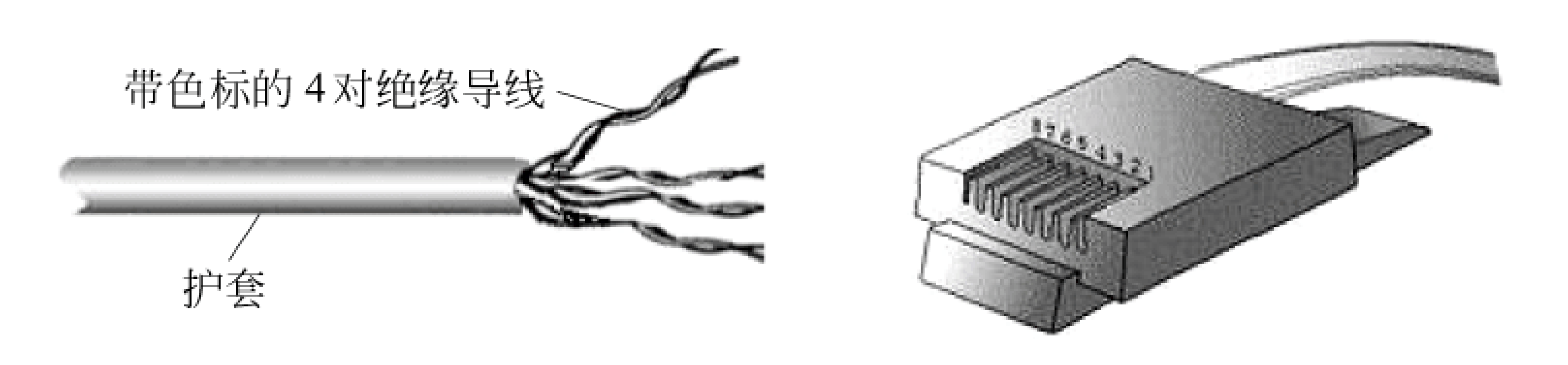


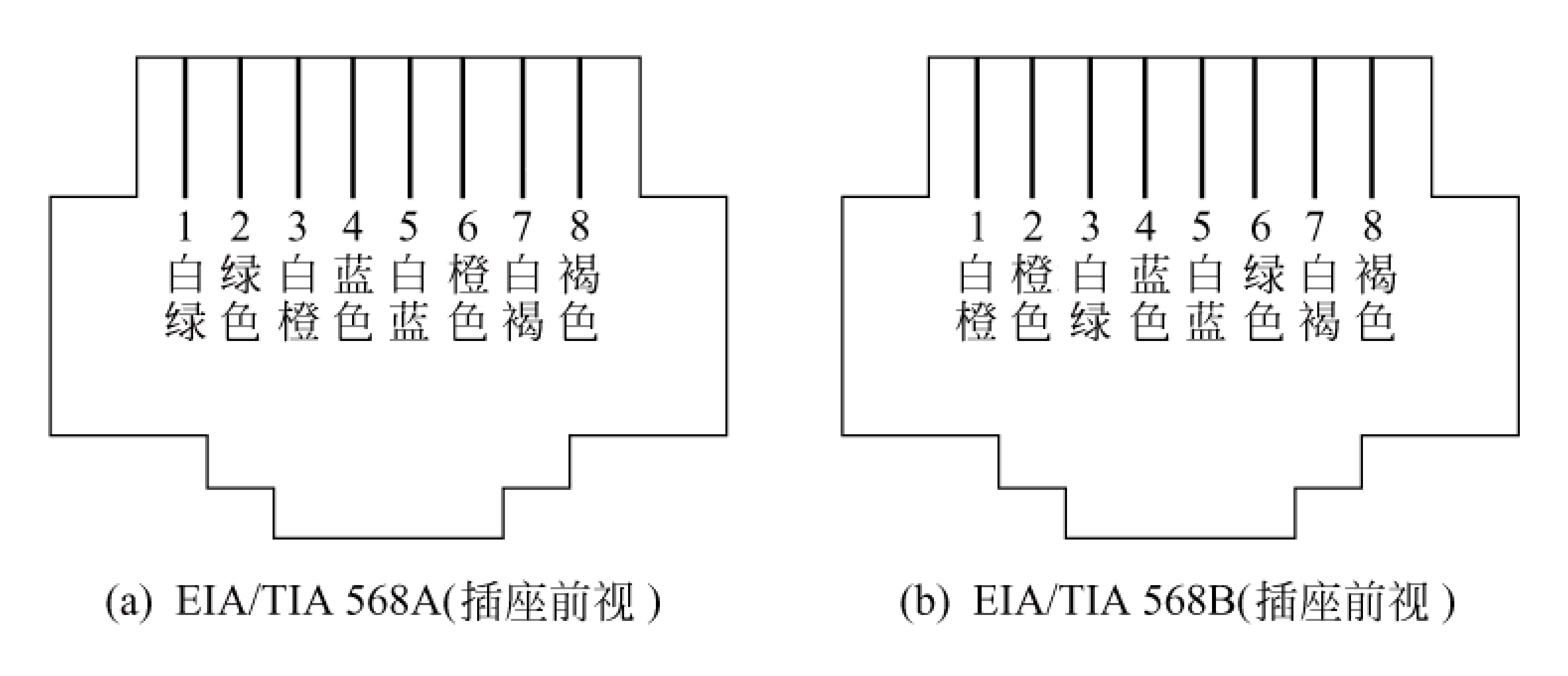
图 1-12　双绞线及 RJ45 接口

双绞线分为屏蔽双绞线（STP）和非屏蔽双绞线（UTP），STP 双绞线内部包了一层皱纹状的屏蔽金属物质，并且多了一条接地用的金属铜丝线，因此它的抗干扰性比 UTP 双绞线强，但价格也要贵很多，阻抗值通常为 150Ω。对于 UTP 双绞线，阻抗值通常为 100Ω，中心芯线 24AMG（直径为 0.5mm），每条双绞线最大传输距离为 100m。

双绞线按其电气特性可分为以下不同的类别：

电气工业协会/电信工业协会(EIA/TIA)约定的 1 类双绞线通常在 LAN 技术中不使用，主要用于模拟语音；2 类可用于综合业务数据网(数据)，如数字话音、IBM3270 等，这类双绞线在 LAN 中很少使用；3 类双绞线是一种 24WG 的 4 对非屏蔽双绞线，符合 EIA/TIA568 标准中确定的 100Ω 水平电缆的要求，可用来进行 10Mbps 和 IEEE 801.3 的 10BaseT 的话音和数据传输；4 类双绞线在性能上比 3 类双绞线有一定改进，适用于包括 16Mbps 令牌环(Token Ring)局域网在内的数据传输速率，可以是 UTP，也可以是 STP；5 类双绞线是 24AWG 的 4 对电缆，比 100Ω 低损耗电缆具有更好的传输特性，并适用于 16Mbps 以上的速率，最高可达 100Mbps；超 5 类电缆系统是在对现有的 UTP 5 类双绞线的部分性能加以改善后出现的系统，不少性能参数，如近端串扰(NEXT)、衰减串扰比(ACR)等都有所提高，但其传输带宽仍为 100MHz，连接方式和现在广泛使用的 RJ45 接插模块相兼容；6 类电缆系统是一个新级别的电缆系统，除了各项参数都有较大提高之外，其带宽将扩展至 200MHz 或更高，连接方式和现在广泛使用的 RJ45 接插模块相兼容；7 类电缆系统是欧洲提出的一种电缆标准，其计划的带宽为 600MHz，但是其连接模块的结构和目前的 RJ45 形式完全不兼容，是一种屏蔽系统。

根据 EIA/TIA 接线标准，双绞线与 RJ45 接头连接时需要 4 根导线通信，两条用于发送数据，两条用于接收数据。RJ45 接口制作有两种标准：EIA/TIA 568A 标准和 EIA/TIA 568B 标准，如图 1-13 所示。



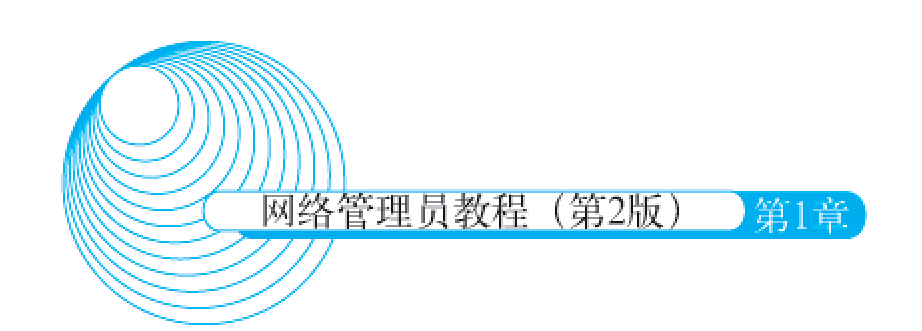
(a) EIA/TIA 568A(插座前视)　(b) EIA/TIA 568B(插座前视)

图 1-13　EIA/TIA RJ45 接口线序

双绞线的制作有两种方法：一是直通线，即双绞线的两个接头都按 568B 线序标准连接；二是交叉线，即双绞线的一个接头按 EIA/TIA 568A 线序连接，另一个接头按 EIA/TIA 568B 线序连接。

3. 光纤

光纤是新一代的传输介质，与铜质介质相比，光纤具有一些明显的优势。因为光纤不会向外界辐射电子信号，所以使用光纤介质的网络无论是在安全性、可靠性还是在传输速率等网络



性能方面都有了很大的提高。

光纤由单根玻璃光纤、紧靠纤芯的包层以及塑料保护涂层组成，如图 1-14(a)所示。为使用光纤传输信号，光纤两端必须配有光发射机和接收机，光发射机执行从电信号到光信号的转换。实现电光转换的通常是发光二极管(LED)或注入式激光二极管(ILD)；实现光电转换的是光电二极管或光电三极管。

根据光在光纤中的传播方式，光纤有两种类型：多模光纤和单模光纤。多模光纤纤芯直径较大，可为 61.5μm 或 50μm，包层外径通常为 125μm。单模光纤纤芯直径较小，一般为 9～10μm，包层外径通常也为 125μm。多模光纤又根据其包层的折射率进一步分为突变型折射率和渐变型折射率。以突变型折射率光纤作为传输媒介时，发光管以小于临界角发射的所有光都在光缆包层界面进行反射，并通过多次内部反射沿纤芯传播。这种类型的光缆主要适用于适度比特率的场合，如图 1-14(b)所示。

多模渐变型折射率光纤使用具有可变折射率的纤芯材料，如图 1-14(c)所示。折射率随离开纤芯的距离增加，导致光沿纤芯的传播接近于正弦波。将纤芯直径减小到一种波长(3～10μm)，可进一步改进光纤的性能，在这种情况下，所有发射的光都沿直线传播，这种光纤称为单模光纤，如图 1-14(d)所示。这种单模光纤通常使用 ILD 作为发光元件，可传输的数据速率为数千兆比特每秒。

从上述 3 种光纤接收的信号看，单模光纤接收的信号与输入的信号最接近，多模渐变型次之，多模突变型接收的信号散射最严重，因而它所获得的速率最低。

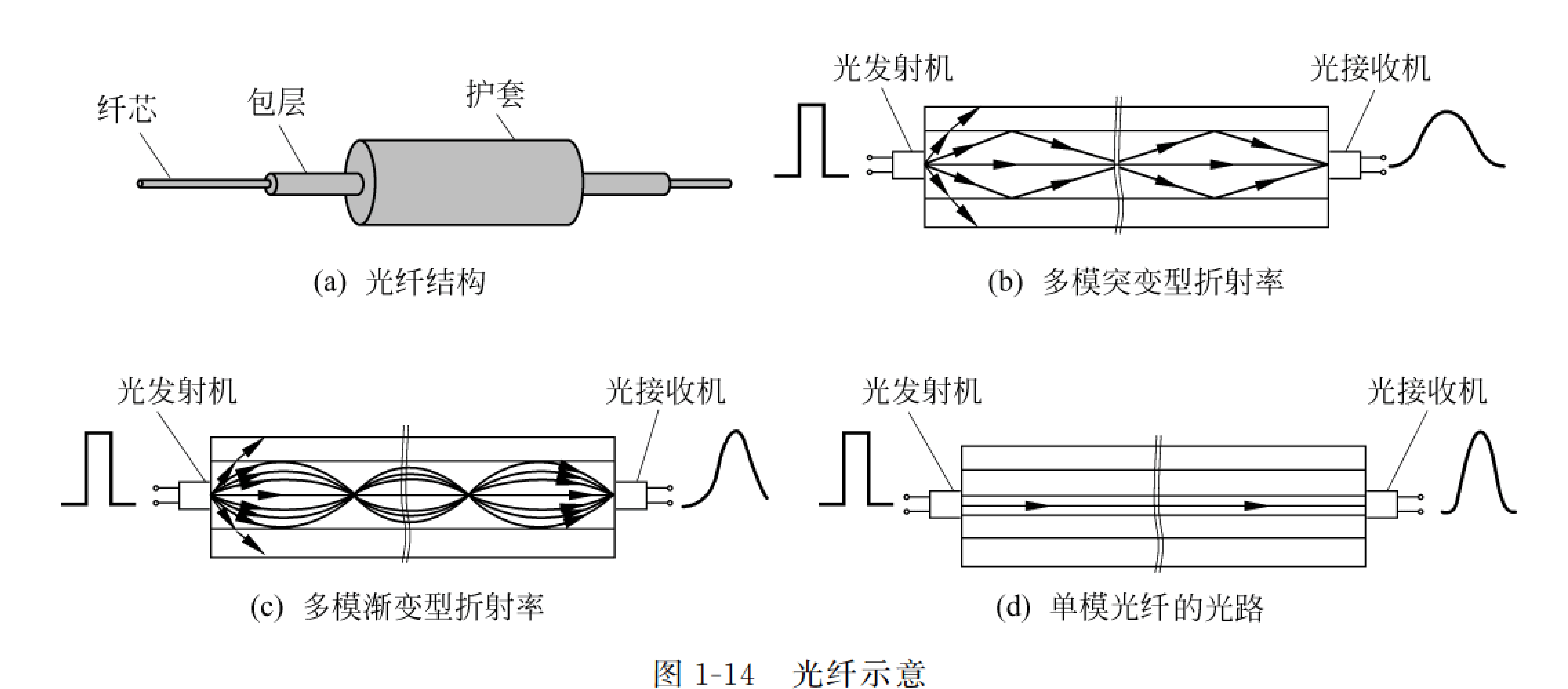


图 1-14 光纤示意

4. 无线传输

上述 3 种传输媒体有一个共同的缺点，那便是都需要一根缆线连接电脑，这在很多场合下

是不方便的。例如，若通信线路需要穿过高山或岛屿或在市区跨越主干道路时就很难敷设，这时利用无线电波在空间自由地传播，可以进行多种通信。尤其近几年，随着移动电话的飞速发展，移动计算机数据通信也变得越来越成熟。

无线传输主要分为无线电、微波、红外线及可见光几个波段，紫外线和更高的波段目前还不能用于通信。国际电信同盟（ITU，International Telecommunications Union）对无线传输所使用的频段进行了正式命名，分别是低频（LF，Low Frequency）、中频（MF，Medium Frequency）、高频（HF，High Frequency）、甚高频（VHF，VeryHF）、特高频（UHF，UltraHF）、超高频（SHF，SuperHF）、极高频（EHF，ExtremelyHF）和目前尚无标准译名的THF（Tuned HF）。

无线电微波通信在数据通信中占有重要地位。微波的频率范围为300MHz～300GHz，但主要使用2～40GHz的频率范围。微波通信主要有两种方式：地面微波接力通信和卫星通信。

由于微波在空间是直线传播，而地球表面是个曲面，因此其传输距离受到限制，一般只有50km左右。若采用100m高的天线塔，传输距离可增大到100km。为实现远距离传输，必须在信道的两个终端之间建立若干个中继站，故称“接力通信”。其主要优点是：频率高，范围宽，因此通信容量很大；因频谱干扰少，故传输质量高，可靠性高；与相同距离的电缆载波通信比，投资少，见效快。缺点是：因相邻站之间必须直视，对环境要求高，有时会受恶劣天气影响，保密性差。

卫星通信是在地球站之间利用位于36 000km高空的同步卫星为中继的一种微波接力通信。每颗卫星覆盖范围达18 000km，通常在赤道上空等距离地放置3颗相隔120°的卫星，就可覆盖全球。和微波接力通信相似，卫星通信也具有频带宽、干扰少、容量大、质量好等优点。另外，其最大特点是通信距离远，基本没有盲区，缺点是传输时延长。

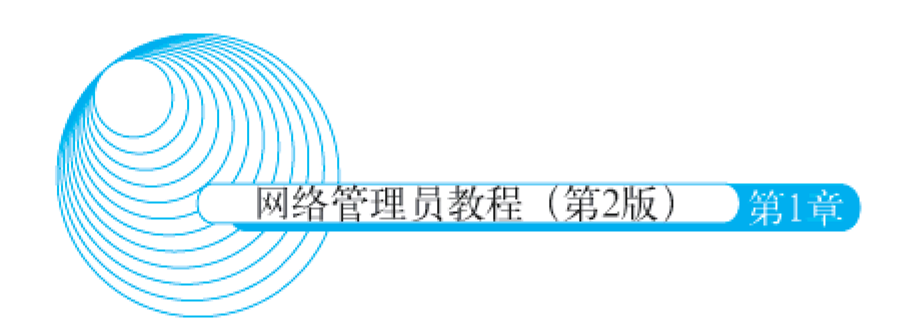
1.3.2 计算机网络互联设备

数据在网络中是以“包”的形式传递的，但不同网络的“包”，其格式也是不一样的。如果在不同的网络间传送数据，由于包格式不同，导致数据无法传送，于是网络间连接设备就充当“翻译”的角色，将一种网络中的“信息包”转换成另一种网络的“信息包”。

信息包在网络间的转换，与OSI的七层模型关系密切。如果两个网络间的差别程度小，则需转换的层数也少。例如以太网与以太网互联，因为它们属于一种网络，数据包仅需转换到OSI的第二层（数据链路层），所需网间连接设备的功能也简单（如网桥）；若以太网与令牌环网相连，数据信息需转换至OSI的第三层（网络层），所需中介设备也比较复杂（如路由器）；如果连接两个完全不同结构的网络TCP/IP与SNA，其数据包需做全部七层的转换，需要的连接设备也最复杂（如网关）。

1. 中继器（Repeater）

在一种网络中，每一网段的传输媒介均有其最大的传输距离，如细缆最大网段长度为



185m，粗缆为 500m，双绞线为 100m，超过这个长度，传输介质中的数据信号就会衰减。如果需要比较长的传输距离，就需要安装一个叫做“中继器”的设备，如图 1-15 所示。中继器可以“延长”网络的距离，在网络数据传输中起到放大信号的作用。数据经过中继器，不需进行数据包的转换。中继器连接的两个网络在逻辑上是同一个网络。

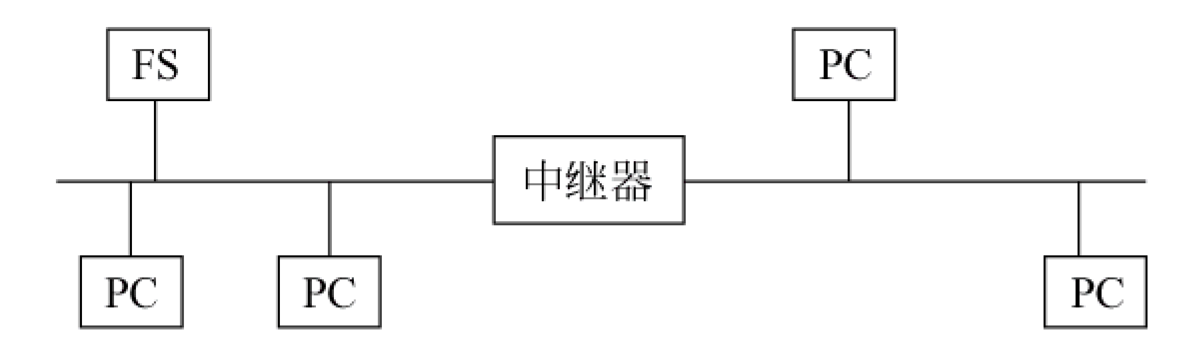


图 1-15　中继器

中继器的主要优点是安装简单，使用方便，价格相对低廉。它不仅起到扩展网络距离的作用，还可以将不同传输介质的网络连接在一起。中继器工作在物理层，对于高层协议完全透明。

2. 网桥（Bridge）

当一个单位有多个 LAN，或一个 LAN 由于通信距离受限无法覆盖所有的节点而不得不使用多个局域网时，需要将这些局域网互联起来，以实现局域网之间的通信。这样就扩展了局域网的范围，扩展局域网最常见的方法是使用网桥。图 1-16 给出了一个网桥的内部结构要点。最简单的网桥有两个端口，复杂些的网桥可以有更多的端口。网桥的每个端口与一个网段（这里所说的网段就是普通的局域网）相连。在图中所示的网桥，其端口 1 与网段 A 相连，而端口 2 则连接到网段 B。

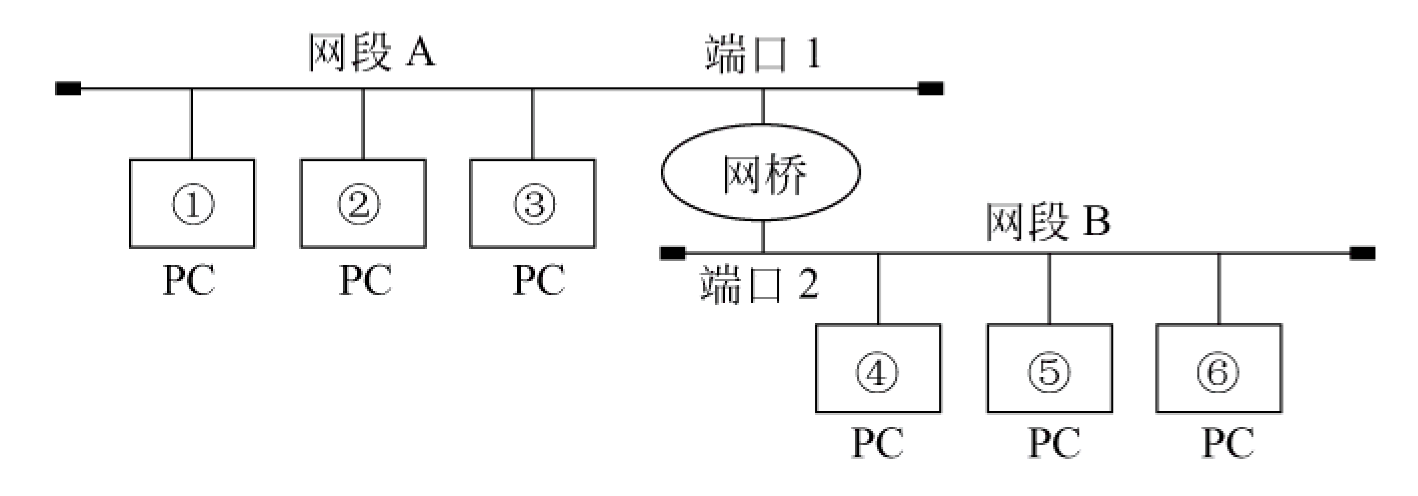


图 1-16　网桥

网桥从端口接收网段上传送的各种帧。每当收到一个帧时，就先存放在其缓冲区中。若此帧未出现差错，且欲发往的目的站地址属于另一个网段，则通过查找站表，将收到的帧送往对应的端口转发出去。否则，就丢弃此帧。因此，仅在同一个网段中通信的帧，不会被网桥转发到另一个网段去，因而不会加重整个网络的负担。例如，设网段 A 的 3 个站的地址分别为①、②和③，而网段 B 的 3 个站的地址分别为④、⑤和⑥。若网桥的端口 1 收到站①发给站②的帧，通过

查找站表，得知应将此帧送回到端口 1。但这表明此帧属于同一个网段上通信的帧，于是丢弃此帧。若端口 1 收到站①发给站⑤的帧，则在查找站表后，将此帧送到端口 2 转发给网段 B，然后再传送给站⑤。

最常见的网桥有透明网桥和源站选路网桥。透明网桥是由各网桥自己来决定路由选择，而局域网上的各站都不管路由选择，这种网桥的标准是 IEEE 801.1(D)。“透明”是指局域网上的每个站并不知道所发送的帧将经过哪几个网桥，而网桥对各站来说是看不见的。透明网桥在收到一个帧时，必须决定是丢弃此帧还是转发此帧，若转发此帧，则应根据网桥中的站表来决定转发到哪个局域网。透明网桥的最大优点就是容易安装，一接上就能工作。但是，网桥资源的利用还不充分。因此，支持 IEEE 801.5 令牌环型网的分委员会就制订了另一个网桥标准，这就是由发送帧的源站负责路由选择，即源站选路(Source Routing)网桥。源站选路网桥假定了每一个站在发送帧时都已清楚地知道发往各个目的站的路由，因而在发送帧时将详细的路由信息放在帧的首部中。

使用网桥可以带来如下好处：

(1) 过滤通信量。网桥可以使局域网的一个网段上各工作站之间的通信量局限在本网段的范围内，而不会经过网桥流到其他的网段去。

(2) 扩大了物理范围，也增加了整个局域网上工作站的最大数目。

(3) 可使用不同的物理层，可互连不同的局域网。

(4) 提高了可靠性。如果把较大的局域网分割成若干较小的局域网，并且每个小的局域网内部的通信量明显高于网间的通信量，那么整个互联网络的性能就变得更好。

当然，网桥也有不少缺点，例如：

(1) 由于网桥对接收的帧要先存储和查找站表，然后才转发，这就增加了时延。

(2) 在 MAC 子层并没有流量控制功能。当网络上负荷很重时，可能因网桥缓冲区的存储空间不够而发生溢出，以致产生帧丢失的现象。

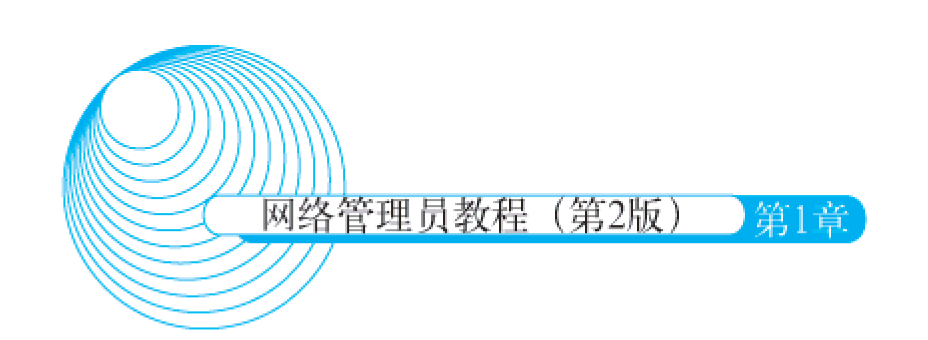
(3) 具有不同 MAC 子层的网段桥接在一起时，网桥在转发一个帧之前，必须修改帧的某些字段的内容，以适合另一个 MAC 子层的要求，这也需要耗费时间。

(4) 网桥只适合于用户数不太多(不超过几百个)和通信量不太大的局域网，否则有时还会产生较大的广播风暴。

3. 路由器(Router)

当两个不同类型的网络彼此相连时，必须使用路由器。例如 LAN A 是令牌环网，LAN B 是以太网(Ethernet)，这时就可以用路由器将这两个局域网连接在一起，如图 1-17 所示。

路由器和网桥进行比较，表面上看，两者均为网络互联，似乎是同一件事情，但两者最本质的差别在于网桥的功能是发生在 OSI 参考模型的第二层(链路层)，而路由器的功能发生在第三



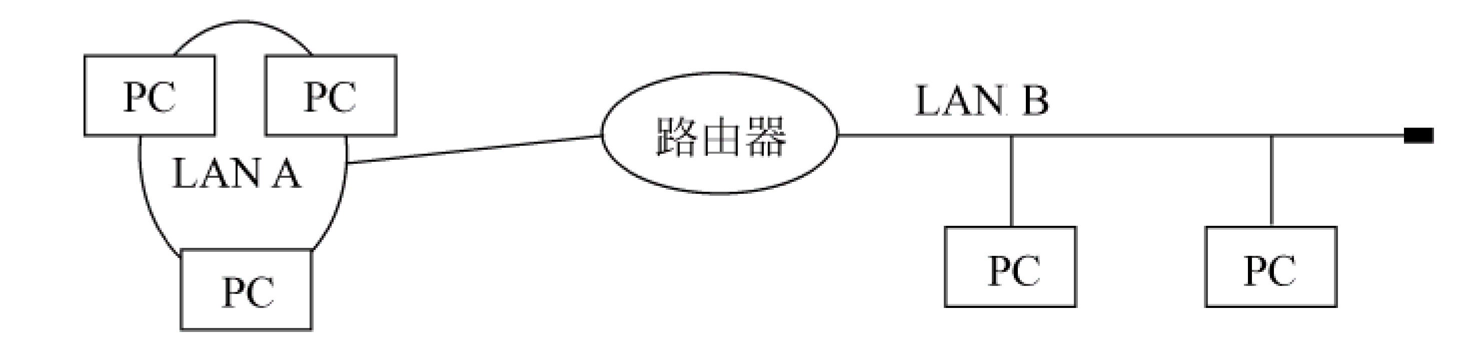


图 1-17　路由器的功能

层(网络层)。由于路由器比网桥高一层,因此智能性更强。它不仅具有传输能力,而且有路径选择能力。当某一链路不通时,路由器会选择一条好的链路完成通信。另外,路由器有选择最短路径的能力。由于路由器的复杂化,其传输信息的速度比网桥要慢,比较适合于大型、复杂的网络连接,也就是说,网桥在把数据从源端向目的端转发时,仅仅依靠链路层的帧头中的信息(MAC 地址)作为转发的依据。而路由器除了分析链路层的信息外,主要以网络层包头中的信息(网络地址)作为转发的依据,但会耗去更多的 CPU 时间,所以路由器的性能从这个意义上讲可能不如网桥。但是正是因为其转发依赖网络协议更高层的信息,所以可以进一步减少其对特定网络技术的依赖性,扩大了路由器的适应范围。再则路由器具有的广播包抑制和子网隔离功能,网桥是不可能具备的。正是这样一种情况使得路由器得到了广泛的应用。

路由器根据分类方法的不同可分为近程路由器和远程路由器;内部路由器和外部路由器;"静态"路由器和"动态"路由器;单协议路由器和多协议路由器等。路由器在工作时需要初始的路径表,它使用这些表来识别其他网络,以及通往其他网络的路径和最有效的选择方法。路由器与网桥不同,它并不是使用路径表来找到其他网络中指定设备的地址,而是依靠其他路由器来完成此任务。也就是说,网桥是根据路径表来转发或过滤信息包的,而路由器是使用它的信息来为每一个信息包选择最佳路径。静态路由器需要管理员来修改所有网络的路径表,一般只用于小型的网络互联;而动态路由器能根据指定的路由协议来完成修改路由器信息。使用这些协议,动态路由器能自动地发送路由信息,所以一般大型的网间连接均使用动态路由器。分段路由器能够在多个网络和介质之间提供网络互联能力,但并不要求在两个网络之间维持永久的连接。与网桥不同,路由器仅在需要时建立新的或附加的连接,用以提供动态的带宽或拆除空闲的连接。此外,当某条路径被拆除或因拥挤阻塞时,路由器提供一条新路径。路由器还能够提供传输的优先权服务,给每一种路由配置提供最便宜或最快速的服务,这些功能都是网桥所没有的。

4. 网关(Gateway)

当连接两个完全不同结构的网络时,必须使用网关。例如以太网与一台 IBM 的大型主机相连,必须用网关来完成这项工作,如图 1-18 所示。

网关不能完全归为一种网络硬件。用概括性的术语来讲,它们应该是能够连接不同网络的

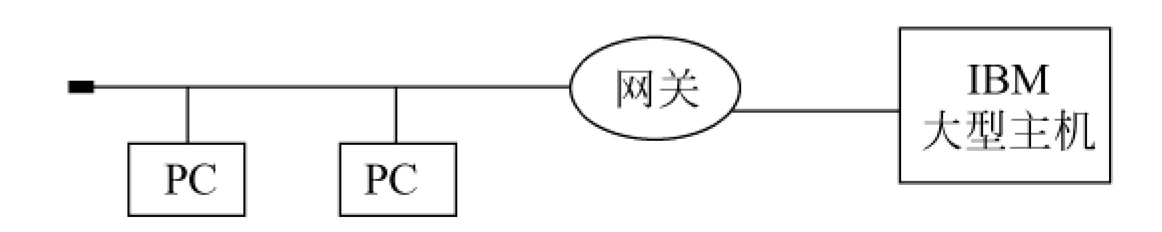


图 1-18　网关的功能

软件和硬件的结合产品。特别要说明的是，它们可以使用不同的格式、通信协议或结构连接起两个系统。网关实际上通过重新封装信息以使它们能被另一个系统读取。为了完成这项任务，网关必须能够运行在 OSI 模型的几个层上。网关必须同应用通信，建立和管理会话，传输已经编码的数据，并解析逻辑和物理地址数据。

网关可以设在服务器、微机或大型机上。由于网关具有强大的功能并且大多数时候都和应用有关，因此比路由器的价格要贵一些。另外，由于网关的传输更复杂，它们传输数据的速度要比网桥或路由器低一些。正是由于网关较慢，它们有造成网络堵塞的可能。然而，在某些场合，只有网关能胜任工作。常见的网关有：

（1）电子邮件网关。该网关可以从一种类型的系统向另一种类型的系统传输数据。例如，电子邮件网关可以允许使用 Eudora 电子邮件的人与使用 Group Wise 电子邮件的人相互通信。

（2）IBM 主机网关。这种网关可以在一台个人计算机与 IBM 大型机之间建立和管理通信。

（3）因特网网关。该网关允许并管理局域网和因特网间的接入，可以限制某些局域网用户访问因特网，反之亦然。

（4）局域网网关。这种网关可以使运行于 OSI 模型不同层上的局域网网段间相互通信。路由器甚至只用一台服务器就可以充当局域网网关。局域网网关也包括远程访问服务器。它允许远程用户通过拨号方式接入局域网。

5．集线器（Hub）

集线器是中继器的一种，其区别仅在于集线器能够提供更多的端口服务，所以集线器又叫多口中继器。集线器主要以优化网络布线结构，简化网络管理为目标而设计的。集线器是对网络进行集中管理的最小单元，像树的主干一样，它是各分枝的汇集点。

通常集线器分为无源集线器、有源集线器和智能集线器。无源集线器只是把相近的多段媒体集中到一起，对它们所传输的信号不作任何处理，而且对它所集中的传输媒体，只允许扩展到最大有效传输距离的一半。有源集线器把相近的多段媒体集中到一起，而且对它们所传输的信号进行整形、放大和转发，并可以扩展传输媒体长度。智能集线器在具备有源集线器功能的同时，还具有网络管理和路径选择功能。

集线器是对网络进行集中管理的最小单元，它只是一个信号放大和中转的设备，不具备自动寻址能力和交换作用，由于所有传到集线器的数据均被广播到与之相连的各个端口，因而容

易形成数据堵塞。集线器源于早期组建10BaseT网络时所使用的集成器。从集线器的作用来看，它不属于网间连接设备，而应叫做网络连接设备。因此它与前面介绍的网桥、路由器、网关等不同，不具备协议翻译功能，而只是分配带宽。例如使用一台 n 个端口的集线器组建10BaseT以太网，每个端口所分配的带宽是 $10Mbps/n$。

以集线器为节点中心的优点是：当网络系统中某条线路或某节点出现故障时，不会影响网上其他节点的正常工作，这就是集线器刚推出时与传统的总线网络的最大的区别和优点，因为它提供了多通道通信，大大提高了网络通信速度。

然而随着网络技术的发展，集线器的缺点越来越突出：用户带宽共享，使带宽受限；广播方式易造成网络风暴；非双工传输使网络通信效率低。正因如此，尽管集线器技术也在不断改进，但实质上就是加入了一些交换机技术，目前集线器与交换机的区别越来越模糊了。随着交换机价格的不断下降，集线器仅有的价格优势已不再明显，它的市场越来越小，已处于淘汰的边缘。尽管如此，集线器对于家庭或者小型企业来说，在经济上还是有一点诱惑力的，特别是应用于家庭几台机的网络中。

6．交换机（Switch）

传统的集线器虽然有许多优点，但分配给每个端口的频带太低了（$10Mbps/n$）。为了提高网络的传输速度，根据程控交换机的工作原理，设计出了交换式集线器（即交换机），如图1-19所示。

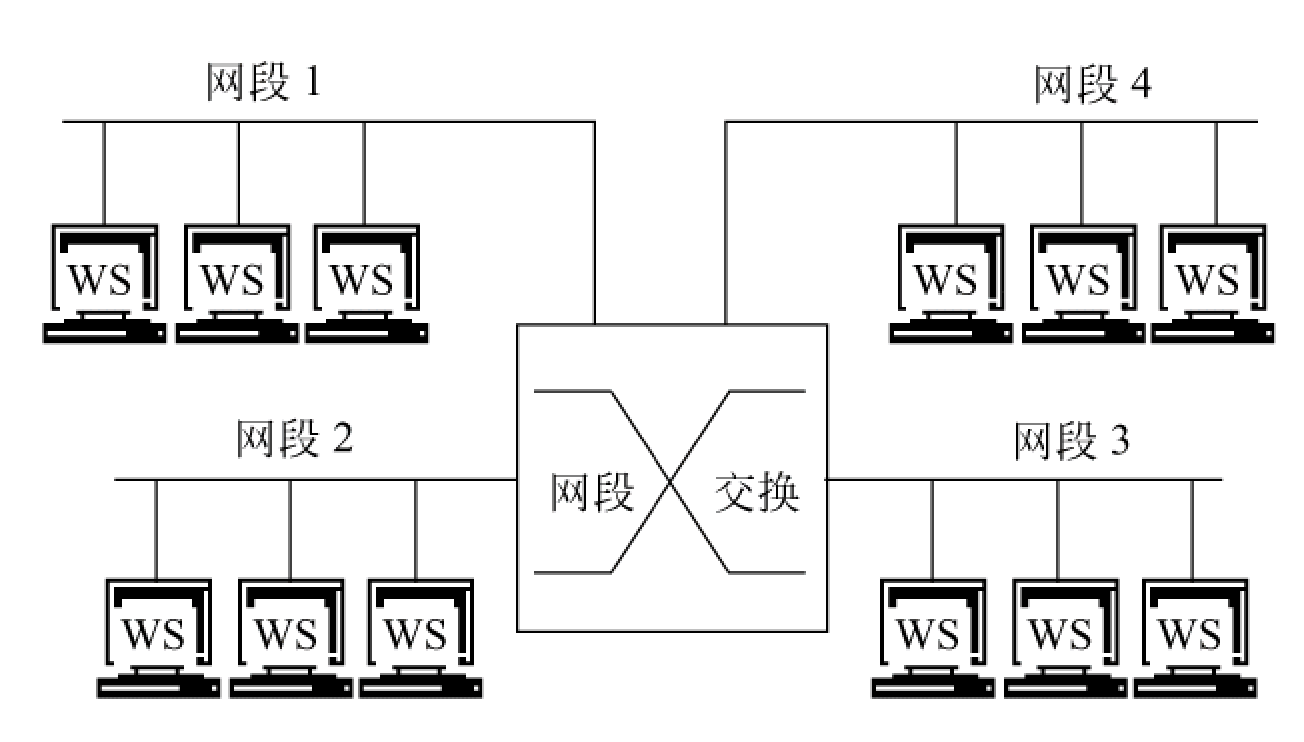


图1-19　交换机示意

交换机提供了另一种提高数据传输速率的方法，且这种方法比FDDI、ATM的成本都要节省许多，交换机能够将以太网的速率提高至真正的10Mbps或100Mbps。目前这种产品已十分成熟，在高速局域网中，已成为必选的设备。

传统式集线器实质上是把一条广播总线浓缩成一个小小的盒子，组成的网络物理上是星型拓扑结构，而逻辑上仍然是总线型的，是共享型的。集线器虽然有多个端口，但同一时间只允许

一个端口发送或接收数据；而交换机则是采用电话交换机的原理，它可以让多对端口同时发送或接收数据，每一个端口独占整个带宽，从而大幅度提高了网络的传输速率。

例如一台8口的10Base T集线器，每个端口所分配到的带宽为10Mbps/8＝1.25Mbps；如果是一台8口的10BaseT交换机，同一时刻可有4个交换通路存在，也就是说可以有4个10Mbps的信道，有4对端口进行数据传输，4个端口分别发送10Mbps的数据，另外4个端口分别接收10Mbps的数据。这样每个端口所分配到的带宽为10Mbps，在理想的满负荷状态下，整个交换机的带宽为10Mbps×8＝80Mbps。

1.3.3 计算机网络接入技术

前面讲述的同轴电缆、双绞线、光纤等传输媒体通常用于构建局域网，但终端远程接入局域网、局域网与局域网远程互联或局域网接入广域网，必须借助公共传输网络。公共传输网络的内部结构和工作机制用户不必关心，用户只须了解公共传输网络提供的接口，如何实现和公共传输网络之间的连接，并通过公共传输网络实现远程端点之间的报文交换。掌握各种公共传输网络的特性，了解公共传输网络和用户网络之间的互联技术是十分重要的。

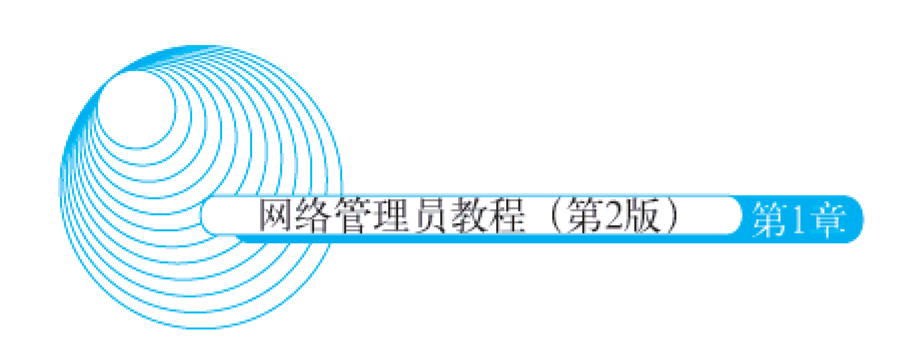
目前，提供公共传输网络服务的单位主要是电信部门，随着电信营运市场的开放，用户可能有较多的选择余地来选择公共传输网络的服务提供者。

公共传输网络基本可以分成两类：电路交换网络和分组交换网络。

电路交换网络的特点是，远程端点之间通过呼叫建立连接，在连接建立期间，电路由呼叫方和被呼叫方专用。经呼叫建立的连接属于物理层链路，只提供物理层承载服务，在两个端点之间传输二进制比特流。分组交换网络提供虚电路和数据包服务。虚电路有永久虚电路和交换虚电路两种。永久虚电路由公共传输网络提供者设置，这种虚电路经设置后，长期存在。交换虚电路需要两个远程端点通过呼叫控制协议建立，在完成当前数据传输后就拆除。虚电路和电路交换的最大区别在于：虚电路只给出了两个远程端点之间的传输通路，并没有把通路上的带宽固定分配给通路两端的用户，其他用户的信息流可以共享传输通路上物理链路的带宽。数据包服务不需要经过虚电路建立过程就可实现报文传送，由于没有在报文的发送端和接收端之间建立传输通路，报文中必须携带源和目的端点地址，而且，公共传输网络的中间节点，必须能够根据报文的目的端点地址选择合适的路径转发报文。当然，呼叫控制协议在建立虚电路时，也必须根据用户设备地址来确定传输通路的两个端点。由于分组交换网络提供的不是物理层的承载服务，所以必须把要求传输的数据信息封装在分组交换网络要求的帧或报文格式的数据字段中才能传输。

1. 公共交换电话网（PSTN，Public Switched Telephone Network）

公共交换电话网是基于标准电话线路的电路交换服务，这是一种最普遍的传输服务，往往



用来作为连接远程端点的连接方法，比较典型的应用有：远程端点和本地 LAN 之间互联、远程用户拨号上网和用作专用线路的备份线路。

由于模拟电话线路是针对话音频率（30～4000Hz）优化设计的，使得通过模拟线路传输数据的速率被限制在 33.4kbps 以内，而且模拟电话线路的质量有好有坏，许多地方的模拟电话线路的通信质量无法得到保证，线路噪声的存在也将直接影响数据传输速率。

2. 窄带综合业务数字网（N-ISDN，Narrowband Integrated Services Digital Network）

当网络的传输系统和交换系统都采用数字技术时，就称为综合数字网（IDN，Integrated Digital Network）。虽然综合数字网与模拟通信网相比是一个不小的进步，但为各种业务分别建网仍不可行，于是人们就设法使各种不同的业务信息经过数字化后，都在一个网络中传输。这就是综合业务数字网 ISDN。由于后来又出现了宽带综合业务数字网 B-ISDN，ITU-T（International Telecommunications Union-Telecom）就把这种由 ISDN 发展而来的，提供端到端的数字连接，支持声音和非声音广泛服务的网络定义为窄带综合业务数字网 N-ISDN。

在 ITU-T 定义的 N-ISDN 标准化组合中，规定有两类接口标准：基本速率接口和一次群速率接口。

基本速率接口提供 2B＋D＝144kbps 的数字通道（每个 B 通道为 64kbps，D 通道为 16kbps），其中两个 B 通道是承载通道，用于完成两端之间数据传输，D 通道是控制通道，用于在用户和 ISDN 交换节点之间传输呼叫控制协议报文。

一次群速率接口有两种速率标准：一种是 30B＋D＝1984kbps（D 通道为 64kbps），加上帧同步和监控信号后，其传输速率为 2048kbps，恰好与欧洲和我国采用的 E1 系统的传输速率相对应；另一种是 23B＋D＝1536kbps，加上帧同步和监控信号后，其传输速率为 1544kbps，恰好与美国和日本采用的 T1 系统的传输速率相对应。

ISDN 用户端和 ISDN 交换节点之间的连接也采用普通双绞线，因此当用户要求把模拟电话线路改成综合业务数字网（ISDN）线路时，不用重新铺设用户线路。虽然模拟拨号服务和 ISDN 服务都属于电路交换服务，但两者还是存在很大差别。由于 ISDN 直接在端到端之间提供数字通道，不但传输速率高，而且可以通过数字通道传输语音、数据和图像信息。由于传输数字信号，信号整形和再生不会引入噪声，这将使 ISDN 线路的传输质量远远高于普通模拟电话线路。

3. 宽带综合业务数字网（B-ISDN，Broadband Integrated Services Digital Network）

随着信息技术的飞速发展，一方面数据传输的速率已越来越快，另一方面各种新的业务不断涌现，N-ISDN 已很难适应用户的宽带需求，因此在 N-ISDN 还未大面积推广使用时，宽带综合业务数字网 B-ISDN 就出现了。B-ISDN 与 N-ISDN 的主要区别是：

（1）B-ISDN 使用一种快速分组交换，叫异步传输模式（ATM，Asynchronous Transfer Mode），而 N-ISDN 使用的是电路交换，只是在传送信令的 D 信道使用分组交换。

（2）B-ISDN 的用户环路和干线都采用光纤，而 N-ISDN 是以目前正在使用的 PSTN 为基础，其用户环路采用双绞线（铜线）。

（3）B-ISDN 采用了虚通路的概念，其传输速率只受用户网络接口的物理比特率的限制，而 N-ISDN 的各通路是预先设置的，如一个 B 通道是 64kbps，当用户不需这么高带宽时，它不能降低，当用户带宽不够时，它又不能升高。

（4）B-ISDN 的传输速率可达每秒百兆甚至千兆比特，而 N-ISDN 的传输速率最多只能为每秒两兆比特。

由于 B-ISDN 的交换方式是异步传输模式 ATM，而 ATM 的物理基础主要是采用了同步数字系列（SDH，Synchronous Digital Hierarchy）标准的光纤传输网络。所以 B-ISDN 与 SDH 的几种标准速率是相同的。

SDH 是 ITU-T 以美国标准同步光纤网（SONET，Synchronous Optical Network）为基础制订的，SDH 的帧结构是一种块状帧，基本信号称为第 1 级同步传递模块 STM-1，相当于 SONET 体系中的 OC3 速率，即为 155.52Mbps。多个 STM-1 复用组成 STM-n，通常用 4 个 STM-1 复用组成 STM-4，相当于 4 个 OC3 复用为 OC12，速率为 622Mbps，4 个 STM-4 复用组成 STM-16，速率为 1.5Gbps，4 个 STM-16 复用组成 STM-64，速率为 10Gbps。

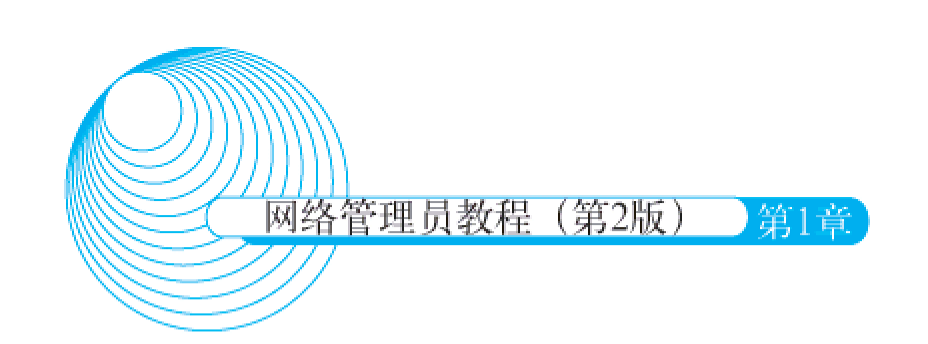
4. X.25 分组交换网

X.25 是 CCITT 制订的在公用数据网上供分组型终端使用的，数据终端设备（DTE，Data Terminal Equipment）与数据通信设备（DCE，Data Communication Equipment）之间的接口建议。

简单地说，X.25 只是一个以虚电路服务为基础的对公用分组交换网接口的规格说明。它动态地对用户传输的信息流分配带宽，能够有效地解决突发性、大信息流的传输问题，分组交换网络同时可以对传输的信息进行加密和有效的差错控制。虽然各种错误检测和相互之间的确认应答浪费了一些带宽，增加了报文传输延迟，但对早期可靠性较差的物理传输线路来说，不失为一种提高报文传输可靠性的有效手段。

但随着光纤越来越普遍地作为传输媒体，传输出错的概率越来越小，在这种情况下，重复地在链路层和网络层实施差错控制，不仅显得冗余，而且浪费带宽，增加报文传输延迟。

由于 X.25 分组交换网络是在早期低速、高出错率的物理链路基础上发展起来的，其特性已不适应目前高速远程连接的要求，因此一般只用于要求传输费用少，而远程传输速率要求又不高的广域网使用环境。虽然现在它已经逐步被性能更好的网络取代，但这个著名的标准在推动分组交换网的发展中作出了巨大贡献。



5. 数字数据网(DDN,Digital Data Network)

DDN是利用数字通道提供半永久性连接电路,向用户提供端到端的中高速率、高质量的数字专用电路,全程实现数字信号透明传输的数据传输网。

DDN可以在两个端点之间建立一条专用的数字通道,通道的带宽可以是$n\times 64$bps,一般$0<n\leqslant 30$。当n为30时,该数字通道就是完整的E1线路,实际带宽可达到2Mbps。DDN专线在租用期间,用户独占该线路的带宽。除传输设备外,DDN干线主要采用光缆、数字微波与卫星信道,所提供的信道是非交换型的半永久电路,其路由通常由电信部门在用户申请时设定,修改并非经常性的。由于DDN采用脉冲编码调制(PCM,Pulse Code Modulation)的数字中继方式,因而传输距离远,可以跨地区、跨国家,与模拟信道相比,具有传输速度快、质量好、性能稳定和带宽利用率高等优点。

DDN网通常由4个部分组成,分别是:

(1) 本地传输系统。主要包括用户设备、用户环路(用户线和用户接入单元)。根据接入DDN的方式(节点机)的不同,用户接入单元可以是频带型或基带型数据传输设备,也可以是多路复用器。如在远程局域网互联时,通常使用基带Modem和路由器。

(2) 复用与交叉连接系统。DDN的复用方式可采用频分多路复用(FDM,Frequency Division Multiplexing)或时分多路复用(TDM,Time Division Multiplexing),目前多采用TDM。交叉连接是指节点内部对复用数字码流通过交叉连接矩阵,以64kbps为单元进行设定的交叉连接。

(3) 局间传输与同步系统。局间利用高速数字中继传送信息,通常设置迂回路由,以提高系统的可靠性。

(4) 网络管理系统。DDN分为干线网和本地网,为便于管理,干线网又分为几个等级。各级通常均要设置网管中心,以对网络进行配置、监控、计费、管理与维护。

DDN目前仍然是许多单位用于实现WAN连接的手段,尤其对于要求持续、稳定、可靠、安全的信息流传输的应用环境更是如此。但对于突发性信息流传输,专用线路或者处于过载状态,或者带宽利用率只达到20%～30%时,其经济性稍差一些。

6. 帧中继(FR,Frame Relay)

帧中继是为了克服传统X.25的缺点,提高其性能而发展出来的一种高速分组交换与传输技术。在一个典型的X.25网络中,分组在传输过程中在每个节点都要进行繁杂的差错检查,而每次差错检查都需要将分组全部接收后才能完成。帧中继则是一种减少节点处理时间的技术。帧中继认为帧的传送基本上不会出错,因此每个节点只要一知道帧的目的地址,也就是只要接收到帧的前6个字节,就立即转发,大大减少了帧在每一个节点的时延,比传统X.25的处理时

间少一个数量级。

帧中继网存在的问题是，一旦出现差错如何处理。按上述方法，只有整个帧被完全接收下来后，节点才能检测到差错，但当节点检测出差错时，该帧的大部分已经转发到下一个节点了。解决这一问题的方法很简单，当检测到有误码的帧后，立即发送终止这次传输的指令，即使帧到达目的节点了，也采用丢弃出错帧的方法。因此，仅当帧中继网络本身的误码率非常低时，帧中继技术才能发挥效能。

帧中继的设计目标主要是针对局域网之间的互联，它以面向连接的方式、合理的数据传输速率和低廉的价格提供数据通信服务。帧中继的主要思想是"虚拟租用线路"。租用 DDN 专线与虚拟租用线路是不同的。租用 DDN 专线期间用户不可能一直以最高传输速率在线路上传送数据，线路利用率不高；由于帧中继采用帧作为数据传送单元，网络的带宽根据用户帧传输的需要，可以采用统计复用的方式动态分配，这样可以充分地利用网络资源，提高了中继带宽的利用率，尤其是对突发信息的适应性比较强。因此，帧中继的虚拟租用线路利用率高，用户费用低（约为 DDN 的 50%）。

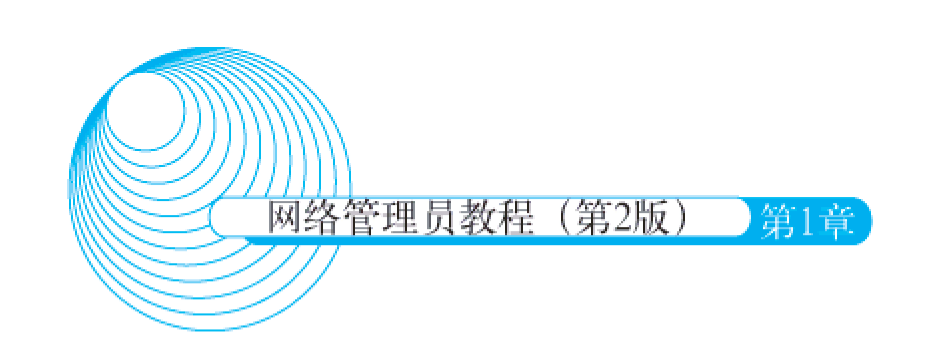
目前，我国已建立了公用帧中继网 ChinaFRN，在现有的 DDN、宽带网上构架和提供帧中继数据传输业务（FRDTS）。

7. 异步传输模式（ATM，Asynchronous Transfer Mode）

电路交换的实时性好，分组交换的灵活性好，B-ISDN 采用了一种结合这两种交换方式优点的交换技术，即 ATM。

ATM 和帧中继都采用了"当正在接收一个帧时，就转发此帧"的快速分组交换技术。那二者有什么区别呢？可以这样理解，快速分组交换技术在实现上有两种方式，它是根据网络中传送的帧长是可变的还是固定的来划分的，当帧长可变时就是帧中继（Frame Relay），当帧长固定（53B）时就是信元中继（Cell Relay）即 ATM。二者的差别是信元中继更适合高速交换，数据传输速率更快。因此，信元中继通常使用在网络中间的核心部分，而帧中继主要使用在网络边界，即如何接入网络。

另外，还要明白 ATM、B-ISDN 和 SDH 之间的关系。概括地讲，B-ISDN 使用的交换方式是 ATM，而 ATM 的物理基础目前主要是采用 SDH 标准的光纤网络。需要说明的是，ATM 的思想最初虽然是针对 B-ISDN 的需求提出的，但最早出现的 ATM 产品却是局域网产品。局域网中的 ATM 技术其传输媒介不仅可以用光纤，还可以用同轴电缆、双绞线等，接口速率也不仅仅限于 SDH 的几种标准速率。因此不能把 ATM 完全等同于 B-ISDN，ATM 是作为一个独立的网络连接技术存在的。但需要指出的是，ATM 的发展并不如当初预期的那样顺利，由于 ATM 技术复杂、设备昂贵，加之快速以太网、千兆以太网的迅速普及，导致 ATM 产品迅速从局域网中淡出，目前仅存在于互联网的高速主干网中。



8．甚小天线地球站（VSAT，Very Small Aperture Terminal）

VSAT是Very Small Aperture Terminal的缩写，直译为“甚小孔径终端”，意译应是“甚小天线地球站”，是20世纪80年代中期开发的一种卫星通信系统。VSAT由于源于传统卫星通信系统，所以也称为卫星小数据站或个人地球站，这里的“小”指的是VSAT系统中小站设备的天线口径小，通常为0.3～1.4m。VSAT具有灵活性强，可靠性高，成本低，使用方便以及小站可直接装在用户端等特点。VSAT系统由一个主站及众多分散设置在各个用户所在地的远端VSAT组成，可不借助任何地面线路，不受地形、距离和地面通信条件限制，主站和VSAT间可直接进行高达2Mbps的数据通信。特别适用于有较大信息量和所辖边远分支机构较多的部门使用。VSAT系统也可提供电话、传真、计算机信息等多种通信业务。该系统由288颗近地轨道卫星构成，每颗星上由路由器通过光通信与相邻卫星连接构成空中互联网。地面服务商接入网关站（双向64Mbps）和一般移动用户（下行64Mbps，上行2Mbps）直接与卫星连接接入。

借助VSAT用户数据终端可直接利用卫星信道与远端的计算机进行联网，完成数据传递、文件交换或远程处理，从而摆脱了本地区的地面中继问题，这在地面网络不发达、通信线路质量不好或难于传输高速数据的边远地区，使用VSAT作为计算机网络接入手段是一种很好的选择。

按照VSAT支持的主要业务类型不同，可分为：以话音业务为主的VSAT系统、以数据业务为主的VSAT系统、以综合业务为主的VSAT系统。

从VSAT网采用的网络结构来看，也可分为3类：星型结构的VSAT系统、网形结构的VSAT系统、星型和网状混合结构的VSAT系统。

9．数字用户线（xDSL，Digital Subscriber Line）

数字用户线xDSL就是利用数字技术对现有的模拟电话用户线进行改造，使它能够承载宽带业务。字母x表示DSL的前缀可以是多种不同的字母，常见的有非对称数字用户线（ADSL，Asymmetrical DSL）、高速数字用户线（HDSL，High Speed DSL）、单对数字用户线（SDSL，Single-line DSL）和甚高速数字用户线（VDSL，Very High Speed DSL）。

xDSL技术的最大特点是使用电信部门已经铺设的双绞线作为传输线路提供高带宽传输速率（从64kbps到52Mbps）。数字用户线也是点对点的专用线路，用户独占线路的带宽。HDSL和SDSL提供对称带宽传输，即双向传输带宽相同，而ADSL和VDSL提供非对称带宽传输，用户向接入设备传输的带宽远远低于接入设备向用户传输的带宽。

数字用户线的主要用途是作为接入线路，把用户网络连接到公共交换网络，如因特网、帧中继、X.25等，目前人们更多的把xDSL作为家庭接入ATM网的接入线路。

xDSL的标准正在制订和完善之中，目前已经投入使用的xDSL技术主要有ADSL和

HDSL。HDSL 虽然是对称传输，但需要两对或三对双绞线，而 ADSL 只需要一对双绞线就可完成双向传输，而且在访问因特网时，用户主要从因特网下载信息，用户传送给因特网的信息并不多，因此不对称传输带宽并没有妨碍 ADSL 作为用户网和公共交换网的接入线路。

10. 宽带网接入

宽带网实际上的名称叫做“IP 城域网”，这是目前较流行的一种接入方式，很多新建的住宅小区都采用这种方式。从技术上讲，它是在城市范围内以多种传输媒介为基础，采用 TCP/IP 协议，通过路由器组网，实现 IP 数据包的路由和交换传输。也可以这样来理解，IP 城域网实际就是一个规模足够大的高速局域网，只不过这个局域网大到可以覆盖整个城市。网内用户连接的不是普通孤立的局域网，而是真正的因特网。每个用户都使用合法的 IP 地址，是真正的因特网用户。网络到用户桌面的带宽远远超过 PSTN、ISDN 所提供的带宽，大部分用户享受的带宽达 10Mbps 或 100Mbps。

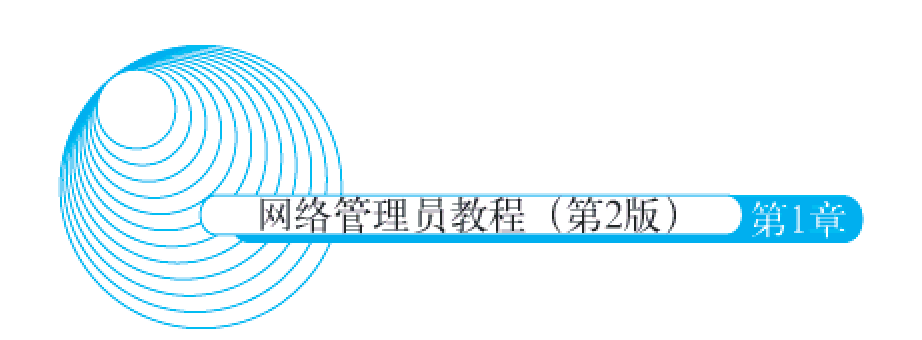
IP 城域网的接入方式目前一般分为 LAN 接入（网线）和 FTTX 接入（光纤）。LAN 接入是指从城域网的节点经过交换器和集线器将网线直接拉到用户的家里，它的优势在于 LAN 技术成熟，网线及中间设备的价格比较便宜，同时可以实现 10Mbps 到 100Mbps 的平滑过渡。

FTTX 接入是指光纤直接拉到用户的家里，即光纤到户（FTTH，Fiber To The Home）或光纤到桌面（FTTD，Fiber To The Desk），由于目前光纤网络产品的价格昂贵，尚未到普及阶段，但它的无限带宽容量却是未来宽带网络发展的方向。

11. HFC 和 Cable Modem

HFC（Hybrid Fiber Coaxial）网是指光纤同轴电缆混合网，它是一种新型的宽带网络，采用光纤到服务区，而在进入用户的“最后 1 千米”采用同轴电缆。最常见的也就是有线电视网络，它比较合理有效地利用了当前的成熟技术，融数字与模拟传输为一体，能够同时提供较高质量和较多频道的传统模拟电视节目、较好性能价格比的电话服务、高速数据传输服务和多种信息增值服务，还可以逐步开展交互式数字视频应用。HFC 网络大部分采用传统的高速局域网技术，但是最重要的组成部分也就是同轴电缆到用户计算机这一段使用了另外的一种独立技术，这就是 Cable Modem。

Cable Modem 编译过来可叫做电缆调制解调器或线缆调制解调器，它是一种将数据终端设备（计算机）连接到有线电视网（CATV，Cable TV），以使用户能够进行数据通信访问因特网等信息资源的设备。它是近几年随着网络应用的扩大而发展起来的，主要用于有线电视网进行数据传输。电缆调制解调器的主要功能是将数字信号调制到射频以及将射频信号中的数字信息解调出来。除此之外，电缆调制解调器还提供标准的以太网接口，部分地完成网桥、路由器、网卡和集线器的功能，因此，它要比传统的 PSTN 调制解调器复杂得多。Cable Modem 与 PSTN



Modem 在原理上都是将数据进行调制后在电缆的一个频率范围内传输，接收时进行解调。不同之处在于 Cable Modem 是通过有线电视 CATV 的某个传输频带进行调制解调的，属于共享介质系统，其他空闲频段仍然可用于有线电视信号的传输。而 PSTN Modem 的传输介质在用户与交换机之间是独立的，即用户独享通信介质。

Cable Modem 提供双向信道：从计算机终端到网络方向称为上行(Upstream)信道，从网络到计算机终端方向称为下行(Downstream)信道。上行信道带宽一般在 200kbps～2Mbps，最高可达 10Mbps，上行信道采用的载波频率范围在 5M～40MHz。下行信道的带宽一般在 3M～10Mbps，最高可达 38Mbps，下行信道采用的载波频率范围在 42M～750MHz。

HFC 有线电视上网的优点就是可以充分利用现有的有线电视网络，不需要再单独架设线路，并且速度比较快，但是它的缺点就是 HFC 网络结构是树型的，Cable Modem 上行 10Mbps、下行 38Mbps 的信道带宽是整个社区用户共享的，一旦用户数增多，每个用户所分配的带宽就会急剧下降，而且共享型网络拓扑结构致命的缺陷就是它的安全性(整个社区属于一个网段)，数据传送基于广播机制，同一个社区的所有用户都可以接收到他人的数据包。

12. 本地多点分配接入系统(LMDS，Local Multipoint Distribution System)

本地多点分配接入系统 LMDS 是 20 世纪 90 年代发展起来的一种宽带无线点对多点接入技术，能够在 3k～5km 的范围内以点对多点的形式进行广播信号传送。在某些国家和地区也称之为本地多点通信系统 LMCS(Local Multipoint Communication System)。所谓"本地"是指：网络的有效距离是单个基站所能够覆盖的范围。LMDS 因为受工作频率和电波传播特性的限制，单个基站在城市环境中所覆盖的半径通常小于 5km；"多点"是指信号从基站到用户端是以点对多点的广播方式传送的，而信号从用户端到基站则是以点对点的方式传送；"分配"是指基站将发出的信号(包括话音、数据及视频业务)分别分配至各个用户。

LMDS 是一种利用高容量点对多点的毫米波微波传输技术。它几乎可以提供任何种类的业务，支持双向话音、数据及视频图像业务，能够实现 64kbps～2Mbps，甚至高达 155Mbps 的用户接入速率，具有很高的可靠性，被称为是一种"无线光纤"技术。

目前，有关 LMDS 标准化工作在 ATM 论坛、DAVIC、ETSI、ITU 等组织的工作下进行，大多数标准化组织都采用 ATM 信元作为基本无线传输机制。LMDS 工作在 24G～38GHz 频段，在不同国家或地区，电信管理部门分配给 LMDS 的具体工作频段及频带宽度有所不同，其中大约有 80％的国家将 27.5G～29.5GHz 定为 LMDS 频段。

13. 无源光网络(PON，Passive Optical Network)

PON 是一种点对多点的光纤传输和接入技术，下行采用广播方式、上行采用时分多址方式，可以灵活地组成树型、星型、总线型等拓扑结构，在光分支点不需要节点设备，只需要安装一个

简单的光分支器即可，因此具有节省光缆资源、带宽资源共享、节省机房投资、设备安全性高、建网速度快、综合建网成本低等优点。PON包括ATM-PON(APON，即基于ATM的无源光网络)和Ethernet-PON(EPON，即基于以太网的无源光网络)两种。

APON传输速率下行为622Mbps或155Mbps，上行为155Mbps。APON与EPON相比，ATM交换机和ATM终端设备昂贵。由于用户终端设备大都是IP设备，采用ATM技术必须将IP包拆分重新封装为ATM信元，这就大大增加了网络的开销，造成网络资源的浪费，但APON的主要特点是对实时业务的支持较好，并能够以较低成本提供服务质量(QoS，Quality of Service)保障。

EPON融合了PON和以太网数据产品的优点，形成了许多独有的优势。EPON系统能够提供高达1Gbps的上下行带宽，由于EPON采用复用技术，支持更多的用户，每个用户可以享受到更大的带宽。EPON系统不采用昂贵的ATM设备和SONET设备，能与现有的以太网相兼容，大大简化了系统结构，成本低，易于升级。由于无源光器件有很长的寿命，因此户外线路的维护费用大为减少。标准的以太网接口可以利用现有的价格低廉的以太网络设备。PON结构本身决定了网络的可升级性比较强，只要更换终端设备，就可以使网络升级到10Gbps或者更高速率。EPON不仅能综合现有的有线电视、数据和话音业务，还能兼容未来业务如数字电视、VoIP、电视会议和VOD等，实现综合业务接入。

1.4 计算机网络协议

1.4.1 OSI体系结构

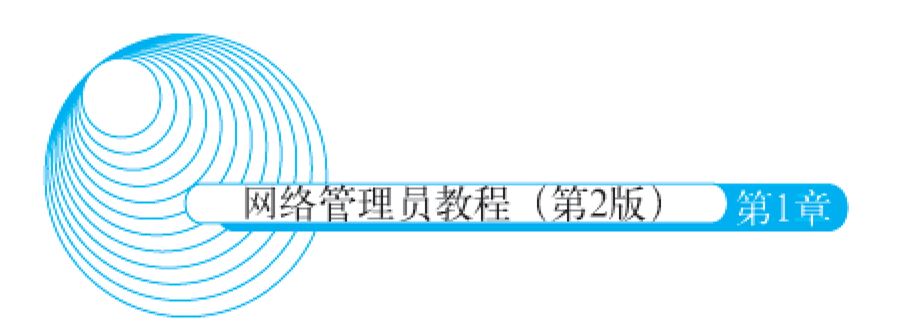
1. 协议的概念

1969年12月，美国国防部高级计划研究署的分组交换网ARPANET投入运行，从此计算机网络的发展进入了一个新的纪元。ARPANET当时仅有4个节点，分别在美国国防部、原子能委员会、麻省理工学院和加利福尼亚。显然在这4台计算机之间进行数据通信仅有传送数据的通路是不够的，还必须遵守一些事先约定好的规则，由这些规则明确所交换数据的格式及有关同步的问题。人与人之间交谈需要使用同一种语言，如果一个人讲中文，另一个人讲英文，那就必须有一个翻译，否则这两人之间的信息无法沟通。计算机之间的通信过程和人与人之间的交谈过程非常相似，只是前者由计算机来控制，后者由参加交谈的人来控制。

计算机网络协议就是通信的计算机双方必须共同遵从的一组约定。例如怎样建立连接，怎样互相识别等。只有遵守这个约定，计算机之间才能相互通信和交流。

通常网络协议由3个要素组成。

(1) 语法，即控制信息或数据的结构和格式；



（2）语义，即需要发出何种控制信息，完成何种动作以及作出何种应答；

（3）同步，即事件实现顺序的详细说明。

2. 开放系统互连参考模型系统结构

ARPANET 的实践经验表明，对于非常复杂的计算机网络而言，其结构最好是采用层次型的。根据这一特点，国际标准化组织 ISO 推出了开放系统互连参考模型（ISO'OSI RM，Open System Interconnect Reference Model）。该模型定义了不同计算机互连的标准，是设计和描述计算机网络通信的基本框架。开放系统互连参考模型的系统结构就是层次式的，共分 7 层，见表 1-1。在该模型中层与层之间进行对等通信，且这种通信只是逻辑上的，真正的通信都是在最底层——物理层实现的，每一层要完成相应的功能，下一层为上一层提供服务，从而把复杂的通信过程分成了多个独立的、比较容易解决的子问题，如图 1-20 所示。

表 1-1　OSI RM

层序号	英文缩写	英文名称	中文名称
7	A	Application Layer	应用层
6	P	Presentation Layer	表示层
5	S	Session Layer	会话层
4	T	Transport Layer	传输层
3	N	Network Layer	网络层
2	DL	Data Link Layer	数据链路层
1	PL	Physical Layer	物理层

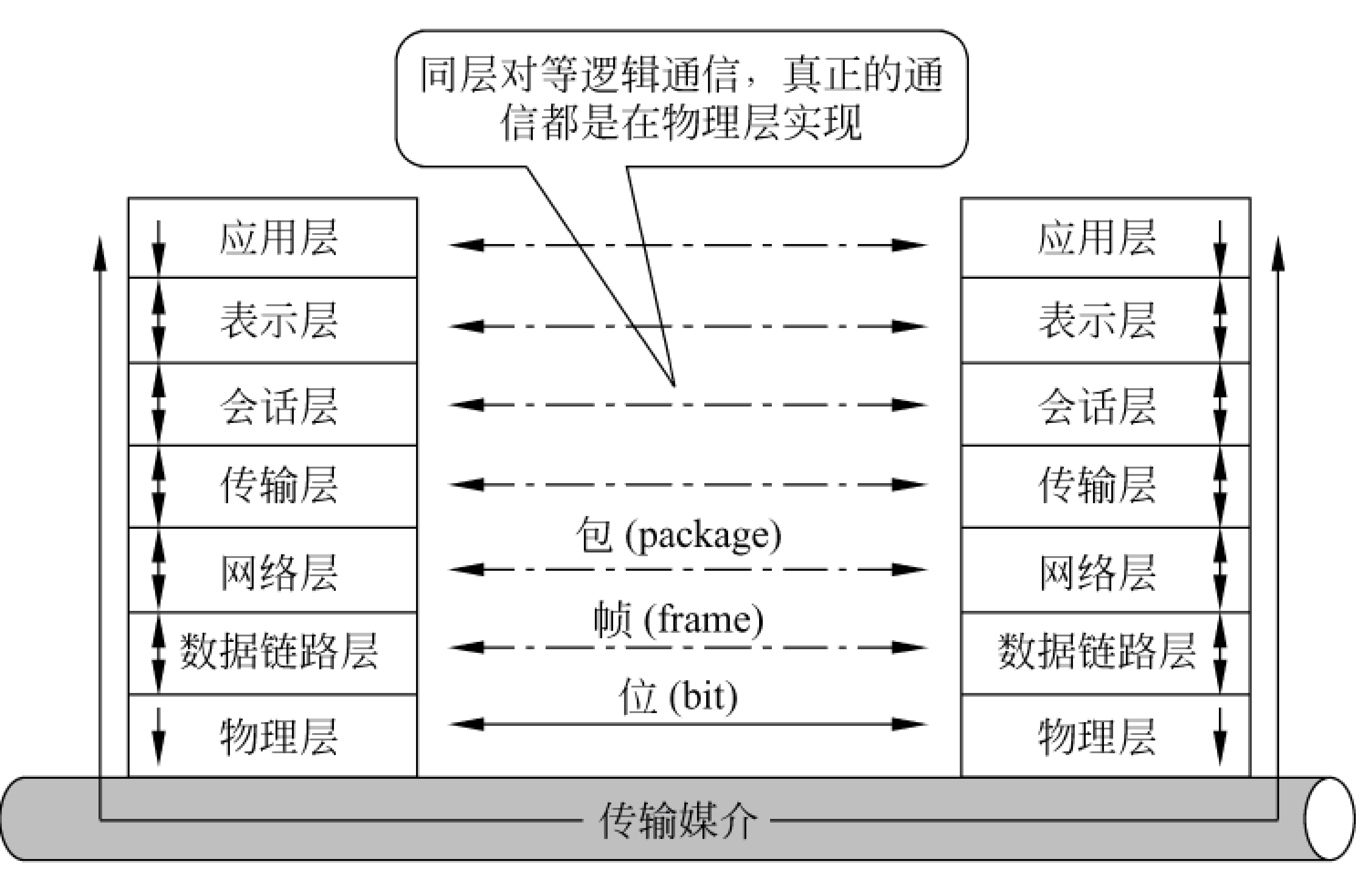


图 1-20　OSI RM 系统结构

从历史上看，在制订计算机网络标准方面，起着很大作用的两个国际组织是：国际标准化组织（ISO，International Standardization Organization）和国际电报电话咨询委员会（CCITT，International Telephone and Telegraph Consultative Committee）。ISO 与 CCITT 工作的领域是不同的，ISO 是一个全球性的非政府组织，是国际标准化领域中一个十分重要的组织。ISO 的任务是促进全球范围内的标准化及其有关活动，以利于国际间产品与服务的交流，以及在知识、科学、技术和经济活动中发展国际间的相互合作。CCITT 现更名为国际电信联盟电信标准化部（ITU-T），其主要职责是完成电联有关电信标准方面的目标，即研究电信技术、操作和资费等问题，出版建议书。虽然 OSI 在一开始是由 ISO 来制订，但后来的许多标准都是 ISO 与 CCITT 联合制订的。CCITT 的建议书 X.200 就是讲解开放系统互连参考模型的。

3. 开放系统互连参考模型各层的功能

1）物理层

物理层是 OSI 分层结构体系中最重要、最基础的一层，它建立在传输媒介基础上，实现设备之间的物理接口。物理层只是接收和发送一串比特流，不考虑信息的意义和信息的结构。

它包括对连接到网络上的设备描述其各种机械的、电气的和功能的规定，还定义电位的高低、变化的间隔、电缆的类型、连接器的特性等。物理层的数据单位是位。

物理层的功能是实现实体之间的按位传输，保证按位传输的正确性，并向数据链路层提供一个透明的位流传输。在数据终端设备、数据通信和交换设备等设备之间完成对数据链路的建立、保持和拆除操作。

2）数据链路层

数据链路层实现实体间数据的可靠传送。通过物理层建立起来的链路，将具有一定意义和结构的信息正确地在实体之间进行传输，同时为其上面的网络层提供有效的服务。在数据链路层中对物理链路上产生的差错进行检测和校正，采用差错控制技术保证数据通信的正确性；数据链路层还提供流量控制服务，以保证发送方不致因为速度快而导致接收方来不及正确接收数据。数据链路层的数据单位是帧。

数据链路层的功能是实现系统实体间二进制信息块的正确传输。为网络层提供可靠无错误的数据信息。在数据链路层中，需要解决的问题包括：信息模式、操作模式、差错控制、流量控制、信息交换过程控制和通信控制规程。

3）网络层

网络层也称通信子网层，是高层协议与低层协议之间的界面层，用于控制通信子网的操作，是通信子网与资源子网的接口。网络层的主要任务是提供路由，为信息包的传送选择一条最佳路径。网络层还具有拥塞控制、信息包顺序控制及网络记账等功能。在网络层交换的数据单元是包。

网络层的功能是向传输层提供服务，同时接受来自数据链路层的服务。其主要功能是实现整个网络系统内连接，为传输层提供整个网络范围内两个终端用户之间数据传输的通路。它涉及到整个网络范围内所有节点、通信双方终端节点和中间节点几方面的相互关系。所以网络层的任务就是提供建立、保持和释放通信连接手段，包括交换方式、路径选择、流量控制、阻塞与死锁等。

4）传输层

传输层建立在网络层和会话层之间，实质上它是网络体系结构中高低层之间衔接的一个接口层。传输层不仅是一个单独的结构层，它还是整个分层体系协议的核心，没有传输层整个分层协议就没有意义。

传输层获得下层提供的服务包括：发送和接收顺序正确的数据块分组序列，并用其构成传输层数据；获得网络层地址，包括虚拟信道和逻辑信道。

传输层向上层提供的服务包括：无差错的有序的报文收发；提供传输连接；进行流量控制。

传输层的功能是从会话层接收数据，根据需要把数据切成较小的数据片，并把数据传送给网络层，确保数据片正确到达网络层，从而实现两层间数据的透明传送。

5）会话层

会话层用于建立、管理以及终止两个应用系统之间的会话。它是用户连接到网络的接口。它的基本任务是负责两主机间的原始报文的传输。

会话层为表示层提供服务，同时接受传输层的服务。为实现在表示层实体之间传送数据，会话连接必须被映射到传输连接上。

会话层的功能包括：会话层连接到传输层的映射、会话连接的流量控制、数据传输、会话连接恢复与释放、会话连接管理、差错控制。

会话层提供给表示层的服务包括：数据交换、隔离服务、交互管理、会话连接同步和异常报告。

会话层最重要的特征是数据交换。与传输连接相似，一个会话分为建立链路、数据交换和释放链路 3 个阶段。

6）表示层

表示层向上对应用层服务，向下接受来自会话层的服务。表示层是为在应用过程之间传送的信息提供表示方法的服务，它关心的只是发出信息的语法与语义。表示层要完成某些特定的功能，主要有不同数据编码格式的转换，提供数据压缩、解压缩服务，对数据进行加密、解密。

表示层为应用层提供的服务包括：语法选择，语法转换等。语法选择是提供一种初始语法和以后修改这种选择的手段。语法转换涉及代码转换和字符集的转换、数据格式的修改以及对数据结构操作的适配。

7）应用层

网络应用层是通信用户之间的窗口，为用户提供网络管理、文件传输、事务处理等服务。其中包含了若干个独立的、用户通用的服务协议模块。网络应用层是 OSI 的最高层，为网络用户之间的通信提供专用的程序。应用层的内容主要取决于用户的各自需要，这一层涉及的主要问题是：分布数据库、分布计算技术、网络操作系统和分布操作系统、远程文件传输、电子邮件、终端电话及远程作业登录与控制等。目前应用层在国际上几乎没有完整的标准，是一个范围很广的研究领域。在 OSI 的 7 个层次中，应用层是最复杂的，所包含的应用层协议也最多，有些还正在研究和开发之中。

1.4.2 TCP/IP 协议

1. 什么是 TCP/IP

前面说过，协议是互相通信的计算机双方必须共同遵从的一组约定。TCP/IP（传输控制协议/网际协议）就是这样的约定，它规定了计算机之间互相通信的方法。TCP/IP 是为了使接入因特网的异种网络、不同设备之间能够进行正常的数据通信，而预先制订的一簇大家共同遵守的格式和约定。该协议是美国国防部高级研究计划署为建立 ARPANET 开发的，在这个协议集中，两个最知名的协议就是传输控制协议（TCP，Transfer Control Protocol）和网际协议（IP，Internet Protocol），故而整个协议集被称为 TCP/IP。之所以说 TCP/IP 是一个协议簇，是因为 TCP/IP 协议包括了 TCP、IP、UDP、ICMP、RIP、TELNET、FTP、SMTP、ARP 等许多协议，对因特网中主机的寻址方式、主机的命名机制、信息的传输规则，以及各种各样的服务功能均做了详细约定，这些约定一起称为 TCP/IP 协议。

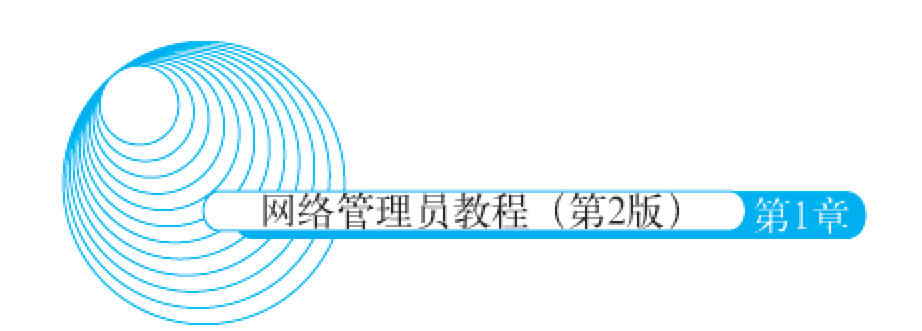
由于因特网在全球范围内迅速发展，因此因特网所使用的协议 TCP/IP 在计算机网络领域中占有十分重要的地位。

2. TCP/IP 协议结构

TCP/IP 协议和开放系统互连参考模型一样，是一个分层结构。协议的分层使得各层的任务和目的十分明确，这样有利于软件编写和通信控制。TCP/IP 协议分为 4 层，由下至上分别是网络接口层、网际层、传输层和应用层，如图 1-21 所示。

最上层是应用层，就是和用户打交道的部分，用户在应用层上进行操作，如收发电子邮件、文件传输等。也就是说，用户必须通过应用层才能表达出他的意愿，从而达到目的。其中简单网络管理协议 SNMP 就是一个典型的应用层协议。

下来是传输层，它的主要功能是：对应用层传递过来的用户信息进行分段处理，然后在各段信息中加入一些附加的说明，如说明各段的顺序等，保证对方收到可靠的信息。该层有两个协议，一个是传输控制协议（TCP），另一个是用户数据包协议 UDP（User Datagram Protocol），



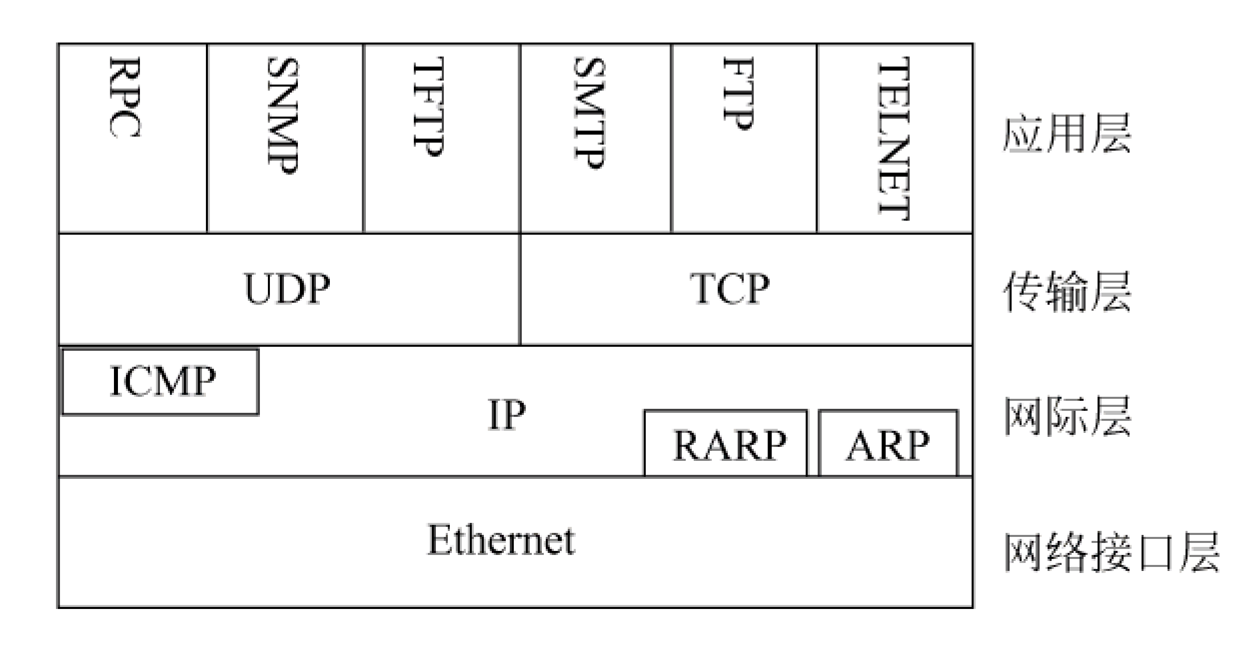


图 1-21　TCP/IP 协议分层结构

SNMP 就是基于 UDP 协议的一个应用协议。

接着是网络层，它将传输层形成的一段一段的信息打成 IP 数据包，在报头中填入地址信息，然后选择好发送的路径。本层的网际协议(IP)和传输层的 TCP 是 TCP/IP 体系中两个最重要的协议。与 IP 协议配套使用的还有 3 个协议：地址解析协议(ARP，Address Resolution Protocol)、逆向地址解析协议(RARP，Reverse Address Resolution Protocol)、因特网控制报文协议(ICMP，Internet Control Message Protocol)。图 1-21 表示出了这 3 个协议和网际协议 IP 的关系。在这一层中，ARP 和 RARP 在最下面，因为 IP 经常要使用这两个协议。ICMP 在这一层的上部，因为它要使用 IP 协议。这 3 个协议将在后面陆续介绍。由于网际协议 IP 可以使互连起来的许多计算机网络能够进行通信，因此 TCP/IP 体系中的网络层常常称为网际层(Internet Layer)。

最底层是网络接口层，也称链路层，其功能是接收和发送 IP 数据包，负责与网络中的传输媒介打交道。

TCP/IP 本质上采用的是分组交换技术，其基本意思是把信息分割成一个个不超过一定大小的信息包传送出去。分组交换技术的优点是：一方面可以避免单个用户长时间占用网络线路，另一方面是在传输出错时不必全部重新传送，只须将出错的包重新传输就可以了。

TCP/IP 规范了网络上的所有通信，尤其是一个主机与另一个主机之间的数据往来格式以及传送方式。可以将数据传送过程形象地理解为：TCP 和 IP 就像两个信封，要传递的信息被划分成若干段，每一段塞入一个 TCP 信封，并在该信封上记录分段号信息，再将 TCP 信封塞入 IP 大信封，发送上网。在接收端，每个 TCP 软件包收集信封，抽出数据，按发送前的顺序还原，并加以校验，若发现差错，TCP 将会要求重发。因此，TCP/IP 在因特网中几乎可以无差错地传送数据。

3. TCP/IP 与 OSI RM 的关系

TCP/IP 协议与开放系统互连参考模型之间的对应关系如图 1-22 所示，其中应用层对应了

OSI 模型的上三层,网络接口层对应了 OSI 模型的下两层。

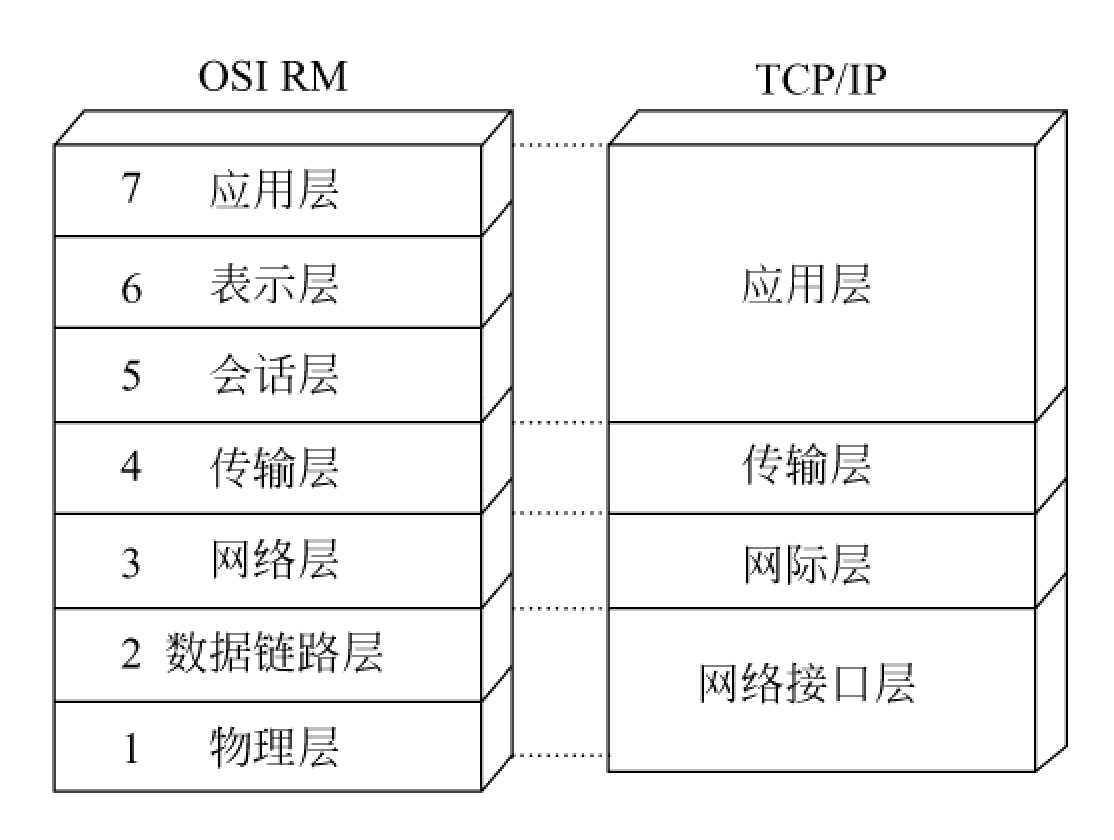


图 1-22 TCP/IP 协议与开放系统互连参考模型之间的对应关系

值得注意的是,在一些问题的处理上,TCP/IP 与 OSI 是很不相同的。例如:

(1) TCP/IP 一开始就考虑到多种异构网(Heterogeneous Network)的互连问题,并将网际协议 IP 作为 TCP/IP 的重要组成部分。但 ISO 和 CCITT 最初只考虑到使用一种标准的公用数据网将各种不同的系统互连在一起。后来,ISO 认识到了网际协议 IP 的重要性,然而已经来不及了,只好在网络层中划分出一个子层来完成类似 TCP/IP 中 IP 的作用。

(2) TCP/IP 一开始就对面向连接服务和无连接服务并重,而 OSI 在开始时只强调面向连接服务,一直到很晚 OSI 才开始制订无连接服务的有关标准。无连接服务的数据包对于互联网中的数据传送以及分组话音通信(即在分组交换网里传送话音信息)都是十分方便的。

(3) TCP/IP 有较好的网络管理功能,而 OSI 到后来才开始考虑这个问题。

4. IP 数据包的格式

IP 数据包的格式能够说明 IP 协议都具有什么功能。在 TCP/IP 的标准中,各种数据格式常常以 32 比特(即 4 字节)为单位来描述。图 1-23 是 IP 数据包的格式。

从图 1-23 可以看出,一个 IP 数据包由首部和数据两部分组成。首部由固定 20 字节的基本首部和 0～40 字节可变长度的任选项组成。下面介绍首部各字段的意义。

(1) 版本:占 4 比特,指 IP 协议的版本。通信双方使用的 IP 协议的版本必须一致。目前使用的 IP 协议版本为 v4(IP version 4),以前的 3 个版本目前已不使用。

(2) IHL:首部长度,占 4 比特,可表示的最大数值是 15 个单位(一个单位为 4 字节),因此 IP 的首部长度的最大值是 60 字节。当 IP 分组的首部长度不是 4 字节的整数倍时,必须利用最后一个补丁字段加以填充。这样,数据部分永远从 4 字节的整数倍时开始,这样在实现起来会比较方便。首部长度限制为 60 字节的缺点是有时(如采用源站选路时)不够用,但这样做的用

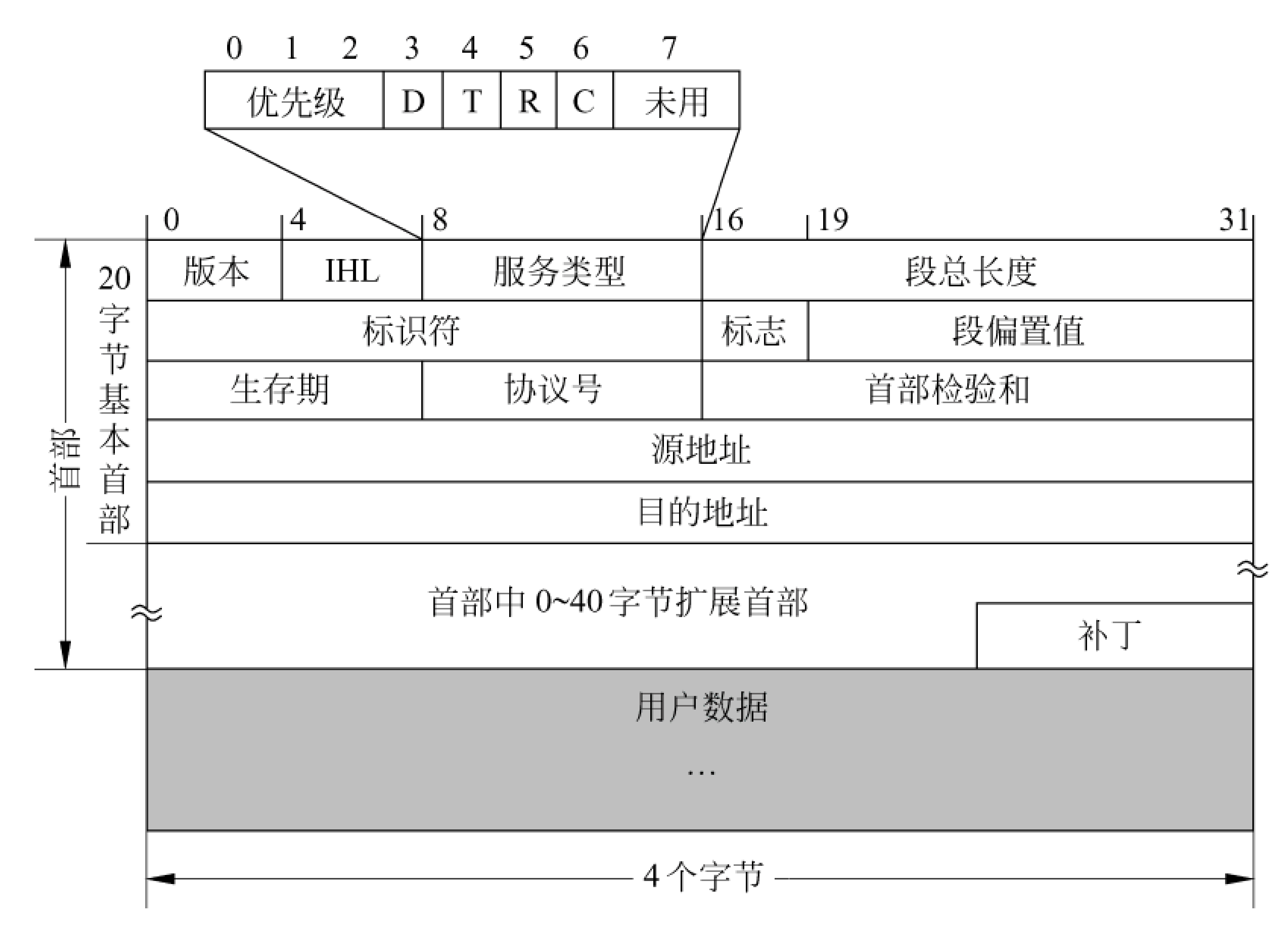


图 1-23　IP 数据包的格式

意是尽量减少额外的开销。

（3）服务类型：占 8 比特，用来获得更好的服务，其意义见图 1-23 的上面部分所示。

服务类型字段的前 3 个比特表示优先级，它可使数据包具有 8 个优先级中的一个。

第 4 个比特是 D 比特，表示要求有更低的时延。

第 5 个比特是 T 比特，表示要求有更高的吞吐量。

第 6 个比特是 R 比特，表示要求有更高的可靠性，即在数据包传送的过程中，被节点交换机丢弃的概率要更小些。

第 7 个比特是 C 比特，是新增加的，表示要求选择费用更低廉的路由。

最后一个比特目前尚未使用。

（4）段总长度：段总长度指首部和数据之和的长度，单位为字节。段总长度字段为 16 比特，因此数据包的最大长度为 65 535 字节，这在当前是够用的。当很长的数据包要分片进行传送时，“总长度”不是指未分片前的数据包长度，而是指分片后每片的首部长度与数据长度的总和。

（5）标识（Identification）：标识字段是为了使分片后的各数据包片最后能准确地重装成为原来的数据包。

注意：这里的“标识”并没有顺序号的意思，因为 IP 是无连接服务的，数据包不存在按序接收的问题。

(6) 标志(Flag)：占 3 比特，目前只有前两个比特有意义。

标志字段中的最低位记为 MF(More Fragment)。MF=1 即表示后面还有分片的数据包；MF=0 表示这已是若干数据包中的最后一个。

标志字段中间的一位记为 DF(Don't Fragment)，只有当 DF=0 时才允许分片。

(7) 段偏置值：该值指出较长的分组在分片后，某个分片在原分组中的相对位置。也就是说，相对于用户数据字段的起点，该片从何处开始。片偏移以 8 字节为偏移单位。

(8) 生存期：TTL(Time To Live)，其单位为秒(s)。生存期的建议值是 32s，但也可设定为 3～4s，甚至为 255s。

(9) 协议号：占 8 比特，协议号字段指出此数据包携带的传输层数据是使用何种协议，以便目的主机的 IP 层知道应将此数据包上交给哪个进程。常用的一些协议和相应的协议字段值(写在协议后面的括弧中)是：UDP(17)、TCP(6)、ICMP(1)、GGP(3)、EGP(8)、IGP(9)、OSPF(89)以及 OSI 的第 4 类传输协议 TP4(29)。

(10) 首部检验和：此字段只检验数据包的首部，不包括数据部分。不检验数据部分是因为数据包每经过一个节点，节点处理机就要重新计算一下首部检验和(一些字段，如寿命、标志、片偏移等都可能发生变化)，如将数据部分一起检验，计算的工作量就太大了。

为了简化运算，检验和不采用 CRC 检验码。IP 检验的计算方法是：将 IP 数据包首部看成为 16 比特字的序列。先将检验的字段置零，将所有的 16 比特字相加后，将和的二进制反码写入检验和字段。收到数据包后，将首部的 16 比特字的序列再相加一次，若首部未发生任何变化，则和必为全 1。否则即认为出差错，并将此数据包丢弃。

(11) 地址：源站 IP 地址字段和目的站 IP 地址字段都各占 4 字节。

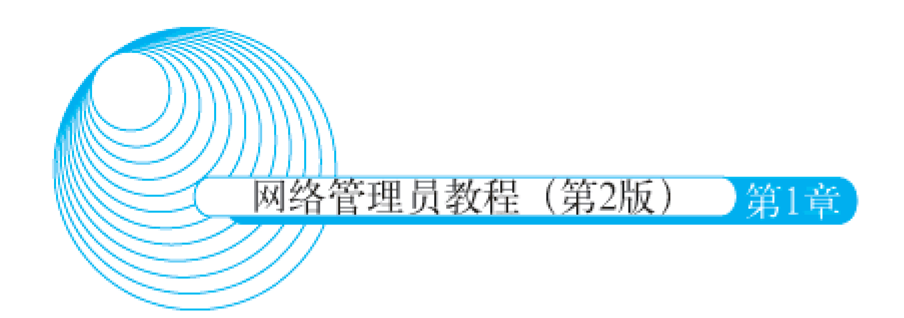
1.4.3 IP 地址

因特网采用了一种通用的地址格式，为因特网中的每一个网络和几乎每一台主机都分配了一个地址，这就使我们实实在在地感觉到它是一个整体。

1. 什么是 IP 地址

接入因特网的计算机与接入电话网的电话相似，每台计算机或路由器都有一个由授权机构分配的号码，称它为 IP 地址。如果某单位电话号码为 85225566，所在的地区号为 10，而我国的电话区号为 0086。那么，这个单位的电话号码完整的表述应该是：0086-10-85225566。这个电话号码在全世界范围内都是唯一的。这是一种很典型的分层结构的电话号码定义方法。

同样，IP 地址也是采用分层结构。IP 地址由网络号与主机号两部分组成。其中，网络号用来标识一个逻辑网络，主机号用来标识网络中的一台主机。一台主机至少有一个 IP 地址，而且这个 IP 地址是全网唯一的，如果一台主机有两个或多个 IP 地址，则该主机属于两个或多个逻辑



网络，一般用做路由器。

在表示 IP 地址时，将 32 位二进制码分为 4 个字节，每个字节转换成相应的十进制，字节之间用“.”来分隔。IP 地址的这种表示法叫做“点分十进制表示法”，显然这比全是 1 和 0 的二进制码容易记忆。例如，有下面的 IP 地址：

10001010 00001011 00000011 00011111

可以记为 138.11.3.31，显然这就方便得多。

2. IP 地址的分类

IP 地址也是采用分层结构。IP 地址由网络号与主机号两部分组成，其中，网络号(net-id)用来标识一个逻辑网络，主机号(host-id)用来标识网络中的一台主机。网络号相同的主机可以直接互相访问，网络号不同的主机需通过路由器才可以互相访问。TCP/IP 协议规定，根据网络规模的大小将 IP 地址分为 5 类(A、B、C、D、E)，如图 1-24 所示。

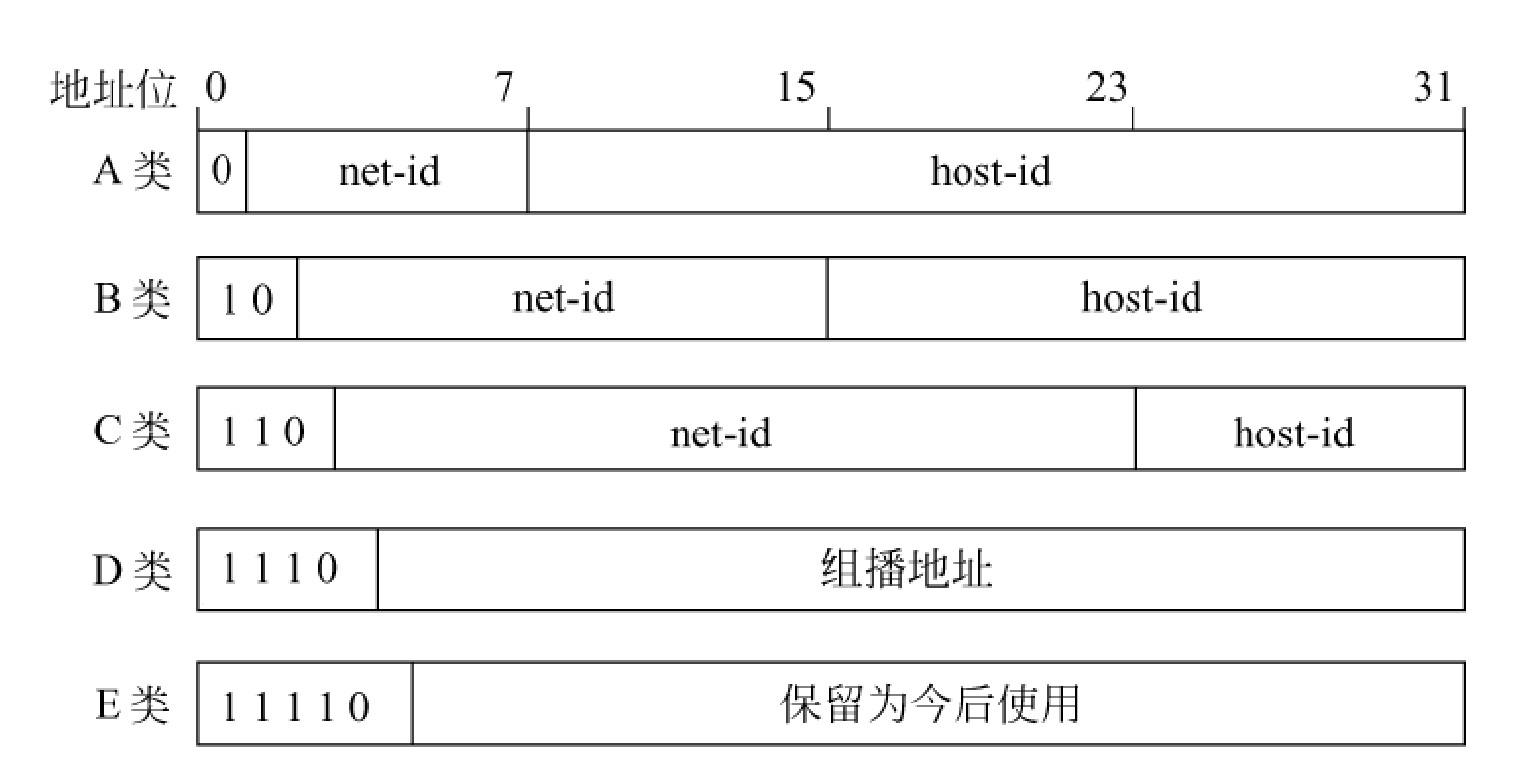


图 1-24　IP 地址的分类

(1) A 类地址：第 1 个字节用做网络号，且最高位为 0，这样只有 7 位可以表示网络号，能够表示的网络号有 $2^7=128$ 个，因为全 0 和全 1 在地址中有特殊用途，所以去掉有特殊用途的全 0 和全 1 地址，这样，就只能表示 126 个网络号，范围是：1～126。后 3 个字节用做主机号，有 24 位可表示主机号，能够表示的主机号有 $2^{24}-2$，约为 1600 万台主机。A 类 IP 地址常用于大型的网络。

(2) B 类地址：前 2 个字节用做网络号，后 2 个字节用做主机号，且最高位为 10，最大网络数为 $2^{14}-2=16382$，范围是：128.1～191.254。可以容纳的主机数为 $2^{16}-2$，约等于 6 万多台主机。B 类 IP 地址通常用于中等规模的网络。

(3) C 类地址：前 3 个字节用做网络号，最后 1 个字节用做主机号，且最高位为 110，最大网络数为 $2^{21}-2$，约等于 200 多万，范围是：192.0.1.0～223.255.254.0，可以容纳的主机数为

2^8-2，等于 254 台主机。C 类 IP 地址通常用于小型的网络。

(4) D 类地址：最高位为 1110，是多播地址，主要是留给因特网体系结构委员会(IAB，Internet Architecture Board)使用的。

(5) E 类地址：最高位为 11110，保留在今后使用。

目前大量使用的 IP 地址仅是 A 至 C 类 3 种。不同类别的 IP 地址在使用上并没有等级之分，不能说 A 类 IP 地址比 B 或 C 类高级，也不能说在访问 A 类 IP 地址时比 B 或 C 类优先级高，只能说 A 类 IP 地址所在的网络是一个大型网络。

3. 子网掩码

IP 地址的设计也有不够合理的地方。例如，IP 地址中的 A 至 C 类地址，可供分配的网络号超过 211 万个，而这些网络上可供使用的主机号的总数则超过 37.2 亿个。初看起来，似乎 IP 地址足够全世界来使用。其实不然。第一，设计者没有预计到微型计算机会普及得如此之快，使得各种局域网和网上的主机数急剧增长。第二，IP 地址在使用时有很大的浪费。例如，某个单位申请到了一个 B 类地址。但该单位只有一万台主机。于是，在一个 B 类地址中的其余 5 万 5 千多个主机号就白白浪费了。因为其他单位的主机无法使用这些号码。为此，设计者在 IP 地址中又增加了一个“子网字段”。

大家知道，一个单位申请到的 IP 地址是这个 IP 地址的网络号 net-id，而后面的主机号 host-id 则由本单位进行分配，本单位所有的主机都使用同一个网络号。当一个单位的主机很多而且分布在很大的地理范围时，往往需要用一些网桥(而不是路由器，因为路由器连接的主机具有不同的网络号)将这些主机互连起来。网桥的缺点较多，例如容易引起广播风暴，同时当网络出现故障时也不太容易隔离和管理。为了使本单位的主机便于管理，可以将本单位所属主机划分为若干个子网(Subnet)，用 IP 地址中的主机号字段中的前若干个比特作为“子网号字段”，后面剩下的仍为主机号字段。这样做就可以在本单位的各子网之间用路由器来互联，因而便于管理。

注意：子网的划分是属于本单位内部的事，在本单位以外看不见这样的划分。从外部看，这个单位仍只有一个网络号。只有当外面的分组进入到本单位范围后，本单位的路由器再根据子网号进行路由选择，最后找到目的主机。若本单位按照主机所在的地理位置来划分子网，那么在管理方面就会方便得多。

图 1-25(a)以 B 类 IP 地址为例，说明了在划分子网时用到的子网掩码(Subnet Mask)的意义。图 1-25(b)表示将本地控制部分再增加一个子网号字段，子网号字段究竟选多长，由本单位根据情况确定。TCP/IP 体系规定用一个 32 比特的子网掩码来表示子网号字段的长度。具体的做法是：子网掩码由一连串的“1”和一连串的“0”组成。“1”对应于网络号和子网号字段，而“0”对应于主机号字段，如图 1-25(c)所示。该子网掩码用点分十进制表示就是 255.255.240.0。

若不进行子网划分，则其子网掩码即为默认值，此时子网掩码中“1”的长度就是网络号的长

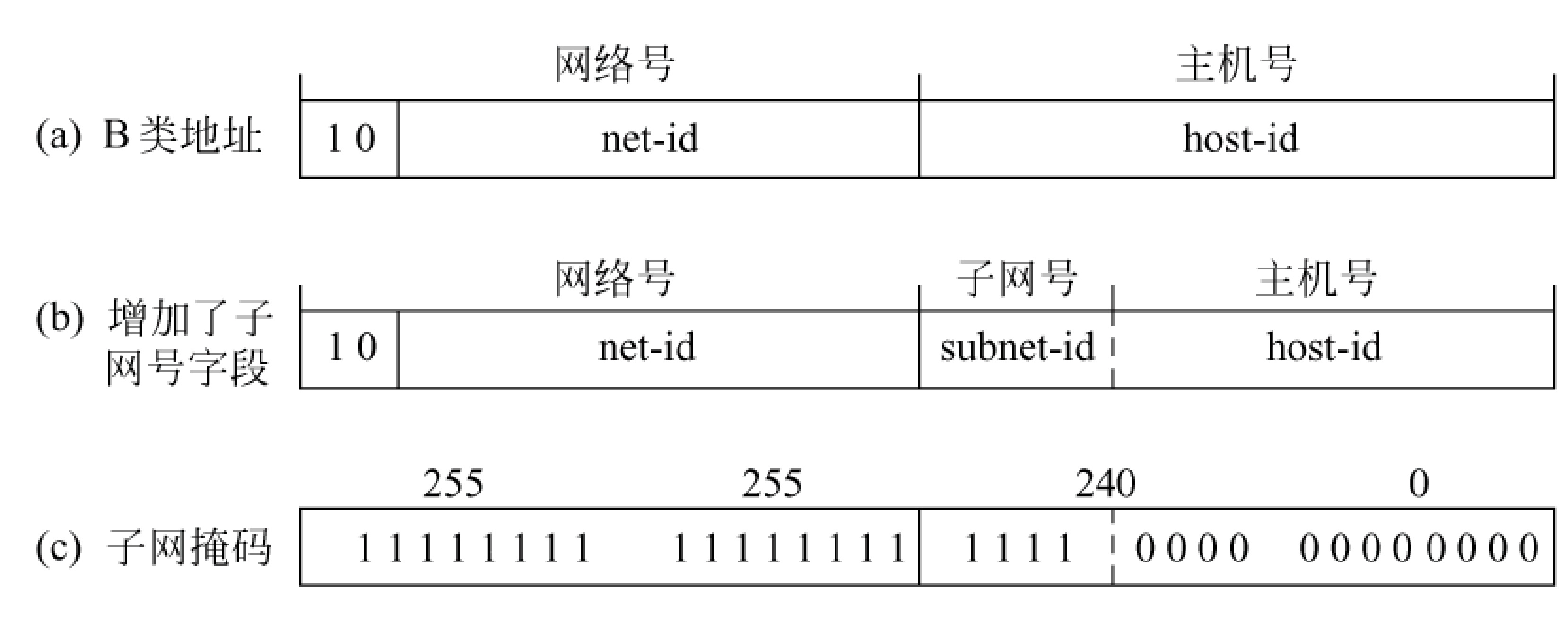


图 1-25　子网掩码的意义

度。因此，对于 A、B 和 C 类 IP 地址，其对应的子网掩码默认值分别为 255.0.0.0、255.255.0.0 和 255.255.255.0。

采用子网掩码相当于采用三级寻址。每一个路由器在收到一个分组时，首先检查该分组的 IP 地址中的网络号。若网络号不是本网络，则从路由表找出下一站地址将其转发出去。若网络号是本网络，则再检查 IP 地址中的子网号。若子网不是本子网，则同样地转发此分组。若子网是本子网，则根据主机号即可查出应从何端口将分组交给该主机。

那么如何判断两个 IP 地址是否是一个子网呢？具体方法是将两个 IP 地址分别和子网掩码做二进制“与”运算。如果得到的结果相同，则属于同一个子网，如果结果不同则不属于同一个子网。

例如：129.47.16.254、129.47.17.01、129.47.32.254、129.47.33.01，这 4 个 B 类 IP 地址如果在默认子网掩码的情况下是属于同一个子网的，但如果子网掩码是 255.255.240.0，则 129.47.16.254 和 129.47.17.01 是属于同一个子网的，而 129.47.32.254、129.47.33.01 则属于另一个子网，如图 1-26 所示。

	网络号		子网号		主机号
子网掩码	11111111	11111111	1111	0000	00000000
129.47.16.254	10000001	00101111	0001	0000	11111110
129.47.17.01	10000001	00101111	0001	0001	00000001
129.47.32.254	10000001	00101111	0010	0000	11111110
129.47.33.01	10000001	00101111	0010	0001	00000001

图 1-26　IP 地址与子网掩码

1.4.4 域名地址

1．域名的概念

通过前面的学习得知，在网上辨别一台计算机的方式是利用 IP 地址。但是一组 IP 地址数字很不容易记忆，因此，需要为网上的服务器取一个有意义又容易记忆的名字，这个名字就叫它域名（Domain Name）。

例如就北京市政府的门户网站“首都之窗”而言，一般使用者在浏览这个网站时，都会输入 www.beijing.gov.cn，而很少有人会记住这台服务器的 IP 地址是多少，www.beijing.gov.cn 就是“北京之窗”的域名，而 210.73.64.10 则是它的 IP 地址，就如同我们在称呼朋友时，一定是叫他的名字，几乎没有人叫对方的身份证号码。

但由于在因特网上真正区分机器的还是 IP 地址，所以当使用者输入域名后，浏览器必须要先去一台有域名和 IP 地址相互对应的数据库的主机中去查询这台计算机的 IP 地址，而这台被查询的主机就称为域名服务器（Domain Name Server），简称 DNS，例如：当输入 www.beijing.gov.cn 时，浏览器会将 www.beijing.gov.cn 这个名字传送到最近的 DNS 服务器去做分析，如果寻找到，则会传回这台主机的 IP 地址，但如果没查到，系统就会提示“DNS NOT FOUND（没找到 DNS 服务器）”，所以一旦 DNS 服务器不工作了，就像是路标完全被毁坏，没有人知道该把资料送到那里。

2．域名的结构

一台主机的主机名由它所属各级域的域名和分配给该主机的名字共同构成。书写的时候，按照由小到大的顺序，顶级域名放在最右面，分配给主机的名字放在最左面，各级名字之间用“.”隔开。

在域名系统中，常见的顶级域名是以组织模式划分的。例如，www.ibm.com 这个域名，因为它的顶级域名为 com，可以推知它是一家公司的网站地址。除了组织模式顶级域名之外，其他顶级域名对应于地理模式。例如，www.tsinghua.edu.cn 这个域名，因为它的顶级域名为 cn，可以推知它是中国的网站地址。表 1-2 显示了常见的顶级域名及其含义。

顶级域的管理权被分派给指定的管理机构，各管理机构对其管理的域继续进行划分，即划分成二级域并将二级域名的管理权授予其下属的管理机构，如此层层细分，就形成了层次状的域名结构，图 1-27 显示了因特网的域名结构。

表 1-2 常见的顶级域名

组织模式顶级域名	含义	地理模式顶级域名	含义
com	商业组织	cn	中国内地
edu	教育机构	hk	中国香港
gov	政府部门	mo	中国澳门
mil	军事部门	tw	中国台湾
net	主要网络支持中心	us	美国
org	上述以外的组织	uk	英国
int	国际组织	jp	日本

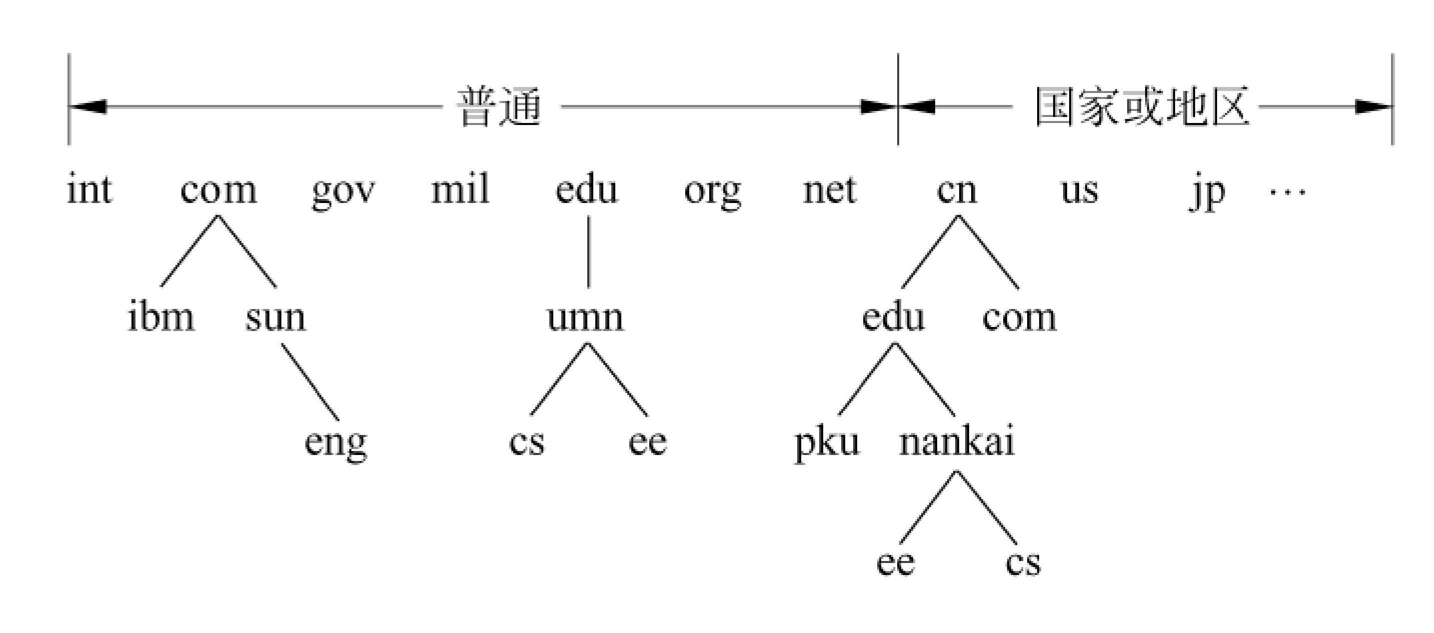


图 1-27 因特网域名结构

因特网的域名由因特网网络协会负责网络地址分配的委员会进行登记和管理。全世界现有 3 个大的网络信息中心：INTER-NIC 负责美国及其他地区，RIPE-NIC 负责欧洲地区，APNIC 负责亚太地区。中国互联网络信息中心（CNNIC，China Internet Network Information Center）负责管理我国顶级域名 cn，负责为我国的网络服务商（ISP）和网络用户提供 IP 地址、自治系统 AS 号码和中文域名的分配管理服务。

3. 域名地址的寻址过程

域名地址的广泛使用是因为它便于记忆，在因特网网络中真正寻找“被叫”时还要用到 IP 地址，因此域名服务器的工作就是专门从事域名和 IP 地址之间的转换翻译。域名地址结构本身是分级的，所以域名服务器也是分级的。

举例说明因特网中的寻址过程，一个国外用户要寻找一台叫 host. edu. cn 的中国主机，其过程如图 1-28 所示。

此用户“呼叫”host. edu. cn，本地域名服务器受理并分析号码；由于本地域名服务器中没有

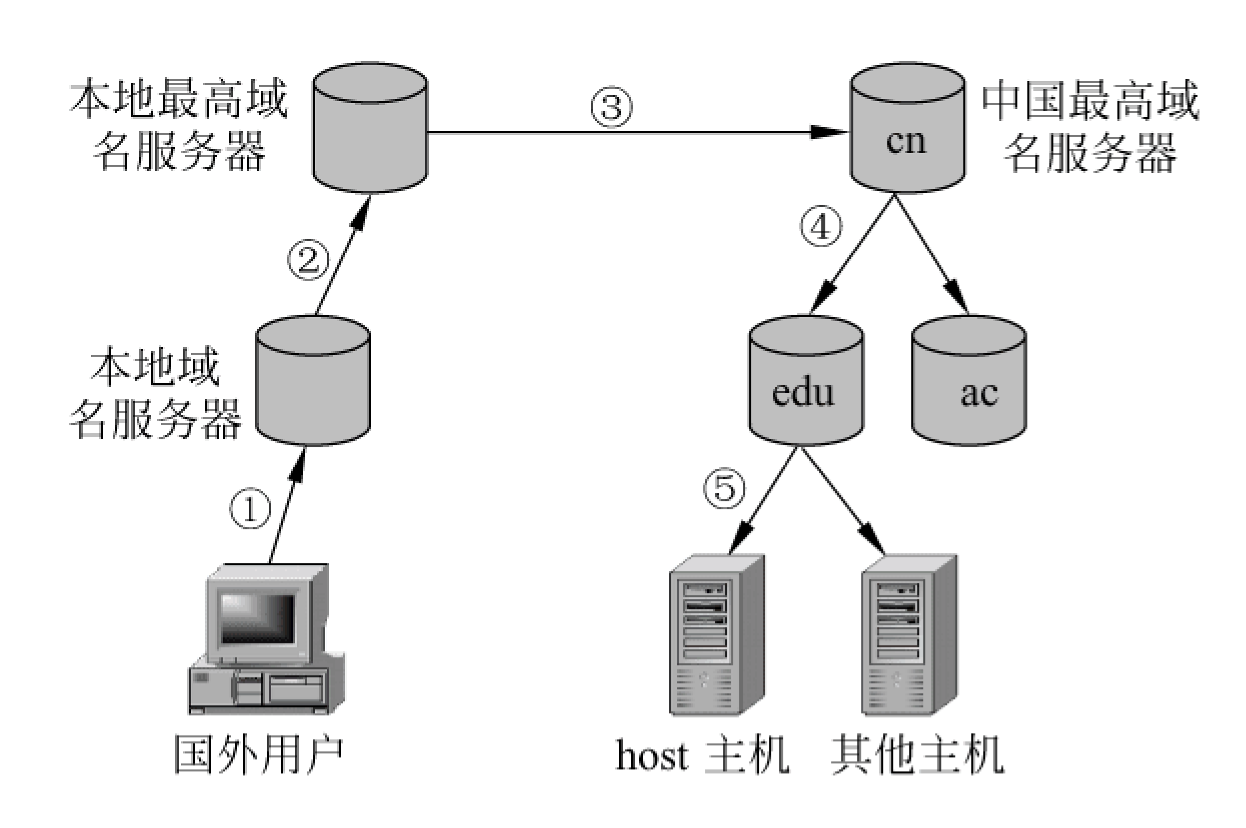


图 1-28 域名地址寻址过程

中国域名资料，必须向上一级查询，图中本地域名服务器向本地最高域名服务器问询；本地最高域名服务器检索自己的数据库，查到 cn 为中国，则指向中国的最高域名服务器；中国最高域名服务器分析号码，看到第二级域名为 edu，就指向 edu 域名服务器，从图中可以看到 ac 域名服务器与 edu 域名服务器是平级的；经 edu 域名服务器分析，找到本域内 host 主机所对应的 IP 地址，就指向名为 host 的主机，这样，一个完整的寻址过程结束。

注意：真正要实现线路上的连接，还是要必须通过通信网络，因此，域名服务器分析域名地址的过程实际就是找到与域名地址相对应的 IP 地址的过程，找到 IP 地址后，路由器再通过选定的端口在电路上构成连接，从此可以看出，域名服务器实际上是一个数据库，它存储着一定范围内主机和网络的域名及相应 IP 地址的对应关系。

1.4.5 IPv6 简介

1. IPv6 的来源

IPv4（IP version 4）标准是 20 世纪 70 年代末期制订完成的。20 世纪 90 年代初期，WWW 的应用导致因特网爆炸性发展，随着因特网应用类型日趋复杂，终端形式特别是移动终端的多样化，全球独立 IP 地址的提供已经开始面临沉重的压力。根据因特网工程任务组（IETF，Internet Engineering Task Force）的估计，基于 IPv4 的地址资源将会在 2005 年开始枯竭。IPv4 将不能满足因特网长期发展的需要，必须立即开始下一代 IP 网络协议的研究。由此，IETF 于 1992 年，成立了 IPNG（IP Next Generation）工作组；1994 年，IPNG 工作组提出了下一代 IP 网络协议（IPv6，IP version 6）的推荐版本；1995 年，IPNG 工作组完成了 IPv6 的协议文本；1995 至 1999 年完成了 IETF 要求的协议审定和测试；1999 年成立了 IPv6 论坛，开始正式分配 IPv6 地址，IPv6 的协议文本成为标准草案。

IPv6 具有长达 128 位的地址空间，可以彻底解决 IPv4 地址不足的问题。由于 IPv4 地址是 32 位二进制，所能表示的 IP 地址个数为 $2^{32}=4\ 294\ 967\ 296\approx 40$ 亿，因而在因特网上约有 40 亿个 IP 地址。由 32 位的 IPv4 升级至 128 位的 IPv6，因特网中的 IP 地址，从理论上讲会有 $2^{128}=3.4\times10^{38}$ 个，如果整个地球表面（包括陆地和水面）都覆盖着计算机，那么 IPv6 允许每平方米有 7×10^{23} 个 IP 地址，如果地址分配的速率是每秒分配 100 万个，则需要 10^{19} 年的时间才能将所有地址分配完毕，可见在想象得到的将来，IPv6 的地址空间是不可能用完的。除此之外，IPv6 还采用分级地址模式、高效 IP 包首部、服务质量、主机地址自动配置、认证和加密等许多技术。

2. IPv6 数据包的格式

IPv6 数据包有一个 40 字节的基本首部（Base Header），其后可允许有零个或多个扩展首部（Extension Header），再后面是数据。图 1-29 所示的是 IPv6 基本首部的格式。每个 IPv6 数据包都是从基本首部开始。IPv6 基本首部的很多字段可以和 IPv4 首部中的字段直接对应。

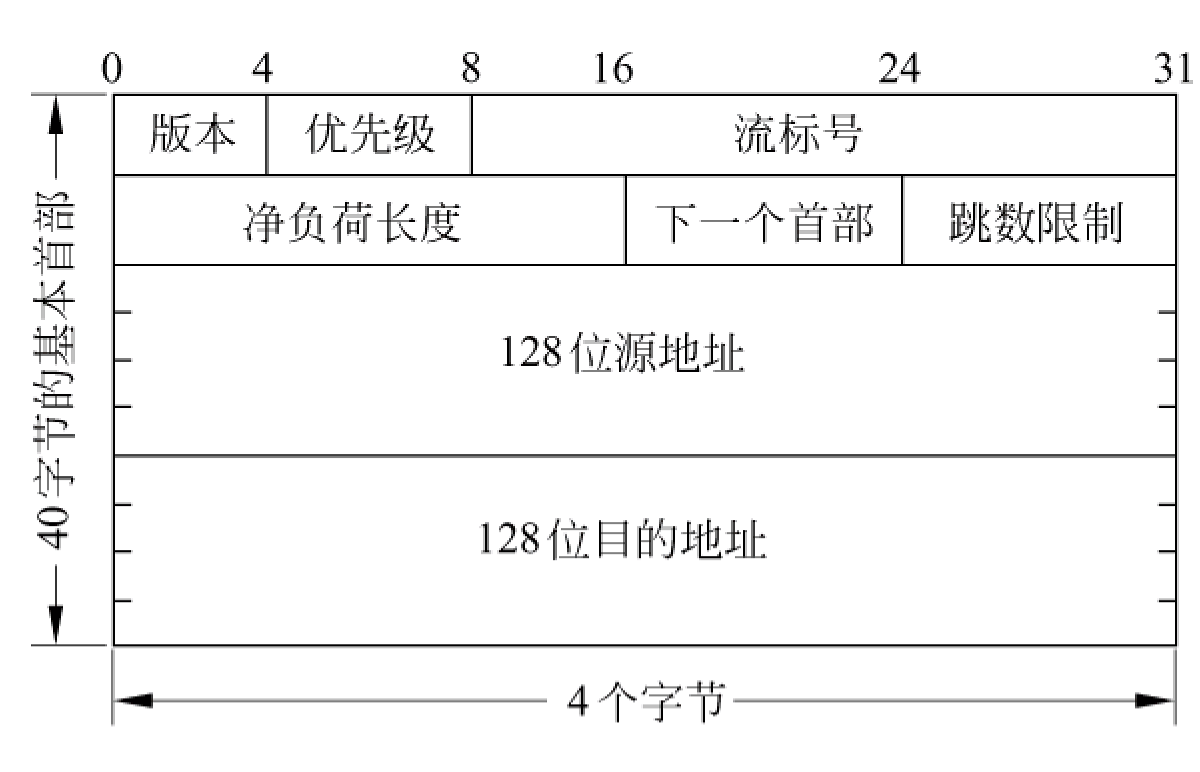


图 1-29 IPv6 基本首部的格式

(1) 版本（Version）：该字段占 4bit，它说明了 IP 协议的版本，对 IPv6 而言，该字段值是 0110，也就是十进制数的 6。

(2) 优先级（Priority）：该字段占 4bit，优先级字段使源站能够指明数据包的流类型。首先，IPv6 把流分成两大类，即可进行拥塞控制的和不可进行拥塞控制的。每一类又分为 8 个优先级。优先级的值越大，表明该分组越重要。对于可进行拥塞控制的业务，其优先级为 0～7。当发生拥塞时，这类数据包的传输速率可以放慢。对于不可进行拥塞控制的业务，其优先级为 8～15。这些都是实时性业务，如音频或视频业务的传输。这种业务的数据包发送速率是恒定的，即使丢掉了一些，也不进行重发。

(3) 流标号（Flow Label）：该字段占 24bit。所谓流就是因特网上从一个特定源站到一个特定目的站（单播或多播）的一系列数据包。所有属于同一个流的数据包都具有同样的流标号。源站在建立流时是在 $2^{24}-1$ 个流标号中随机选择一个流标号。流标号 0 保留作为指出没有采

用流标号。源站随机地选择流标号并不会在计算机之间产生冲突，因为路由器在将一个特定的流与一个数据包相关联时，使用的是数据包的源地址和流标号的组合。

从一个源站发出的具有相同非零流标号的所有数据包，都必须具有相同的源地址和目的地址，以及相同的逐跳选项首部（若此首部存在）和路由选择首部（若此首部存在）。这样做的好处是当路由器处理数据包时，只要查一下流标号即可，而不必查看数据包首部中的其他内容。任何一个流标号都不具有特定的意义，源站应将它希望各路由器对其数据包进行的特殊处理写明在数据包的扩展首部中。

(4) 净负荷长度（Payload Length）：该字段占16bit，此字段指明除首部自身的长度外，IPv6数据包所载的字节数。可见一个IPv6数据包可容纳64K字节长的数据。由于IPv6的首部长度是固定的，因此没有必要像IPv4那样指明数据包的总长度（首部与数据部分之和）。

(5) 下一个首部（Next Header）：该字段占8bit，标识紧接着IPv6首部的扩展首部的类型。这个字段指明在基本首部后面紧接着的一个首部的类型。

(6) 跳数限制（Hop Limit）：该字段占8bit，此字段用来防止数据包在网络中无限期地存在。源站在每个数据包发出时即设定某个跳数限制。每一个路由器在转发数据包时，要先将跳数限制字段中的值减1。当跳数限制的值为零时，就要将此数据包丢弃。这相当于IPv4首部中的生存期字段，但比IPv4中的计算方法要简单些。

(7) 源站IP地址：该字段占128bit，是数据包的发送站的IP地址。

(8) 目的站IP地址：该字段占128bit，是此数据包的接收站的IP地址。

3. IPv6的地址表示

一般来讲，一个IPv6数据包的目的地址可以是以下3种基本类型地址之一。

(1) 单播（Unicast）：单播就是传统的点对点通信。

(2) 多播（Multicast）：多播就是一点对多点的通信，数据包交付到一组计算机中的每一个。IPv6没有采用广播的术语，而是将广播看作多播的一个特例。

(3) 任播（Anycast）：这是IPv6增加的一种类型。任播的目的站是一组计算机，但数据包在交付时只交付给其中的一个，通常是距离最近的一个。

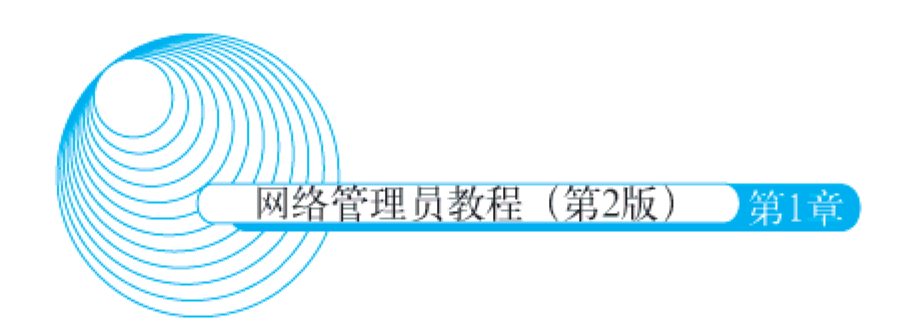
为了使地址的表示简洁些，IPv6使用冒号十六进制记法（Colon Hexadecimal Notation，简写为colon hex），它把每个16bit用相应的十六进制表示，各组之间用冒号分隔。例如：

686E：8C64：FFFF：FFFF：0：1180：96A：FFFF

冒号十六进制记法允许零压缩（Zero Compression），即一连串连续的零可以用一对冒号所取代，例如：

FF05：0：0：0：0：0：0：B3

可以定成：



FF05：：B3

为了保证零压缩有一个清晰的解释，建议中规定，在任一地址中，只能使用一次零压缩。该技术对已建议的分配策略特别有用，因为会有许多地址包含连续的零串。

另外，冒号十六进制记法可结合有点分十进制记法的后缀。这种结合在 IPv4 向 IPv6 的转换阶段特别有用。例如，下面的串是一个合法的冒号十六进制记法：

0：0：0：0：0：0：128.10.1.1

在这种记法中，虽然为冒号所分隔的每个值是一个 16bit 的量，但每个点分十进制部分的值则指明一个字节的值。使用零压缩即可得出：

：：128.10.1.1

4. IPv6 的变化

1）采用了全新的地址管理方式

在 IPv4 中，地址是用户拥有的。也就是说，一旦用户从某机构处申请到一段地址空间，他就永远使用该地址空间。ISP 必须在路由表中为每个用户的网络号维护一条记录。随着用户数量的增加，会出现大量无法会聚的特殊路由，导致产生路由表爆炸现象。即使无类别域间路由（CIDR）也不能处理这种情况。IPv6 的地址管理方式是，从用户拥有变成了 ISP 拥有。全局网络号由因特网地址分配机构（IANA）分配给各 ISP，用户的全局网络地址只是 ISP 地址空间的子集。当用户改变接入的 ISP 时，全局网络地址更新为改变后 ISP 提供的地址。这样 ISP 能有效地控制路由信息，从而避免路由表爆炸现象的出现。

2）提供了地址自动配置机制

为了避免手工配置 IP 地址的繁琐，IPv6 提供了地址自动配置机制，使主机能自动生成地址，实现了主机的即插即用功能。路由器在地址自动配置中发挥巨大的作用，它定时在子网里广播，广播报文中包括主机能使用的地址前缀的所有信息，如前缀值、生命期等。主机收到该报文后，按照一定规则在本地生成主机标识符，把它和地址前缀连接，从而形成主机地址。为了保证主机地址的唯一性，IPv6 定义了重复地址检测过程，每当生成地址时，必须反复执行生成和检测过程，直到得到唯一的地址。

3）增加了邻机发现协议（NDP）

IPv6 定义了邻机发现协议（NDP），可进行通用的地址解析和可达性检测。IPv4 中 ARP 是独立的协议，负责 IP 地址到 MAC 地址的转换，对不同的链路层协议要定义不同的 ARP。IPv6 把 ARP 纳入 NDP 并运行于 ICMP 上，使 ARP 更具有一般性，包括更多的内容，而且不用为每种链路层协议定义一种 ARP。可达性检测的目的是确认相应 IP 地址代表的主机或路由器是否还能收发报文，IPv4 没有统一的解决方案。IPv6 的 NDP 中定义了可达性检测过程，保证 IP 报文不会发送给“黑洞”。

4）简化了数据包的首部

IPv6 的另一个变化是对数据包的首部进行了简化，尽量避免那些很少使用的字段占用空间。IPv4 数据包的首部有 13 个字段，而 IPv6 则只包含 7 个字段，其基本首部在源和目的地址采用了 128 位地址的情况下，也才只有 40 个字节，可见效率之高。这使得路由器处理分组的速度加快，大大提高了吞吐率。

IPv6 数据包首部中的“下一个首部”域，它指向数据包首部的扩展部分，这样便可以在非常简单的结构里提供灵活的可选特征。同 IPv4 一样，IPv6 允许数据包包含可选的控制信息，但在 IPv4 头中必需的字段现在只是 IPv6 的选项。而且，选项出现在扩展头部中，使路由器可以简单地跳过选项，加速了分组处理的过程。

5）增强了安全性

IPv6 利用数据包首部的扩展部分可以提供路由器级的安全性。IPv6 中强制性的安全性包括两方面的内容。一方面，IPv6 数据包的接收者可以要求发送者首先利用 IPv6 认证头（数据包首部的扩展部分）进行“登录”，然后才接收数据包，这种登录是算法独立的，可以有效地阻止网络“黑客”的攻击。另一方面，利用 IPv6 的封闭安全头（数据包首部的扩展部分）加密数据包，这种加密也是算法独立的，这意味着可以安全地在因特网上传输敏感数据，不用担心被第三方截取。另外，IPv6 还定义了 ISAKMP-OAKLEY 协议，其基础是 Diff-Hellmann 算法。规定首先进行证书交换，用以确认对方的地址真伪，然后进行带验证过程的密钥交换，防止密钥交换被中介拦截。协议中也定义了相应的手段允许协商加密参数，以及 AH 和 ESP 的用法。

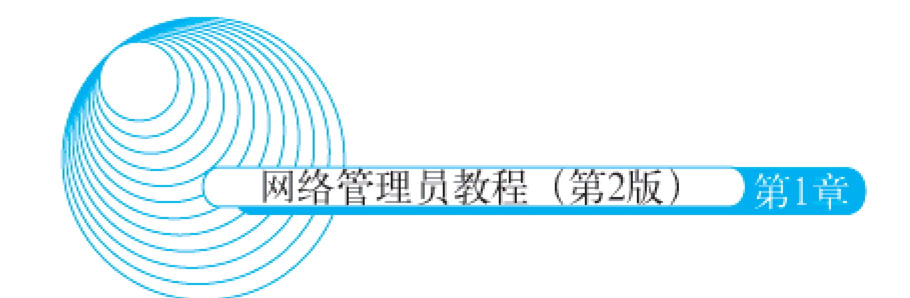
6）增强了移动性

移动 IPv6（MIPv6）在新功能和新服务方面可提供更大的灵活性。每个移动设备设有一个固定的家地址（Home Address），这个地址与设备当前接入因特网的位置无关。当设备在“家”以外的地方使用时，通过一个转交地址来提供移动节点当前的位置信息。发送给移动节点的 IPv6 包，就透明地路由到该节点的转交地址处。对通信节点和转交地址之间的路由进行优化，就会使网络的利用率更高。

基于移动 IPv6 协议集成的 IP 层移动功能具有很重要的优点。尤其是在移动终端数量持续上涨的今天，这些优点更加突出。尽管 IPv4 中也存在一个类似的移动协议，但二者之间存在着本质的区别：移动 IPv4 协议不适用于数量庞大的移动终端。

5. IPv4 向 IPv6 的过渡

尽管 IPv6 比 IPv4 具有明显的先进性，但是 IETF 认识到，要想在短时间内将因特网和各个企业网络中的所有系统全部从 IPv4 升级到 IPv6 是不可能的，也就是说，IPv6 与 IPv4 系统在因特网中长期共存是不可避免的现实。为此，IETF 制订了推动 IPv4 向 IPv6 过渡的方案，其中包括 3 个机制：兼容 IPv4 的 IPv6 地址、双 IP 协议栈和基于 IPv4 隧道的 IPv6。



兼容 IPv4 的 IPv6 地址是一种特殊的 IPv6 单点广播地址，一个 IPv6 节点与一个 IPv4 节点可以使用这种地址在 IPv4 网络中通信。双 IP 协议栈是在一个系统（如一个主机或一个路由器）中同时使用 IPv4 和 IPv6 两个协议栈。这类系统既拥有 IPv4 地址，也拥有 IPv6 地址，因而可以收发 IPv4 和 IPv6 两种 IP 数据包。与双 IP 协议栈相比，基于 IPv4 隧道的 IPv6 是一种更为复杂的技术，它是将整个 IPv6 数据包封装在 IPv4 数据包中，由此实现在当前的 IPv4 网络中 IPv6 节点与 IPv4 节点之间的 IP 通信。基于 IPv4 隧道的 IPv6 实现过程分为 3 个步骤：封装、解封和隧道管理。封装是指由隧道起始点创建一个 IPv4 包头，将 IPv6 数据包装入一个新的 IPv4 数据包中。解封是指由隧道终节点移去 IPv4 包头，还原初始的 IPv6 数据包。隧道管理是指由隧道起始点维护隧道的配置信息，如隧道支持的最大传输单元（MTU）的尺寸等。

IPv6 是一个建立可靠的、可管理的、安全和高效的 IP 网络的长期解决方案。尽管 IPv6 的实际应用之日还需耐心等待，不过，了解和研究 IPv6 的重要特性以及它针对目前 IP 网络存在的问题而提供的解决方案，对于制订企业网络的长期发展计划，规划网络应用的未来发展方向，都是十分有益的。

第2章 因特网及其应用

2.1 因特网入门

2.1.1 因特网简介

大家已经知道，Internet 的中文名字叫因特网，它是当今世界上最大的信息网，是全人类最大的知识宝库之一。通过因特网，用户可以实现全球范围内的电子邮件、WWW 信息查询、电子邮件、文件传输、网络娱乐、语音与图像通信服务等功能。目前，因特网已经成为覆盖全球的信息基础设施之一。

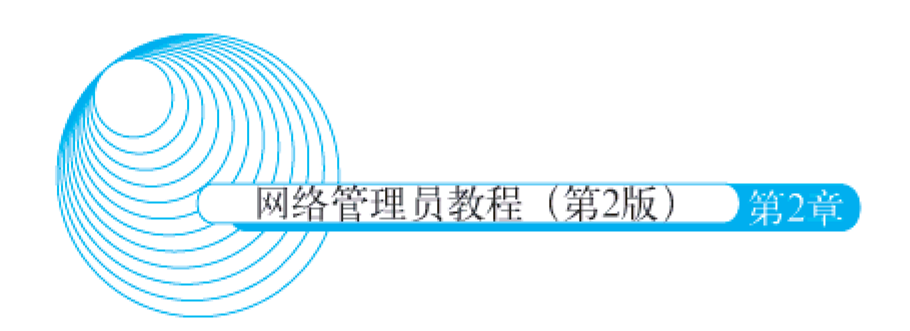
因特网的前身是 1969 年美国国防部高级研究计划署（ARPA，Advanced Research Projects Agency）的军用实验网络，名字为 ARPANET，起初只有 4 台主机，分别位于美国国防部、原子能委员会、加州理工大学和麻省理工大学，其设计目标是当网络中的一部分因战争原因遭到破坏时，其他主机仍能正常运行。20 世纪 80 年代初期，ARPA 和美国国防部通信局成功地研制了用于异构网络的 TCP/IP 协议并投入使用。1986 年在美国国家科学基金会（NSF，National Science Foundation）的支持下，通过高速通信线路把分布在各地的一些超级计算机连接起来，经过十几年的发展形成了因特网的雏形。

因特网连接了分布在世界各地的计算机，并且按照统一的规则为每台计算机命名，制订了统一的网络协议 TCP/IP 来协调计算机之间的信息交换。任何人、任何团体都可以加入到因特网。对用户开放、对服务提供者开放是因特网获得成功的重要原因。TCP/IP 协议就像是在因特网中使用的世界语，只要因特网上的用户都使用 TCP/IP 协议，大家就能方便地进行交谈。

在因特网上你“是谁”并不重要，重要的是你提供了什么样的信息。每个自愿连入因特网的主机都有各种类型的信息资源。无论是跨国公司的服务器，还是个人入网的计算机，都仅仅是因特网数千万网站中的一个节点；无论是总统、明星还是平民，都只能是因特网数千万网民中的一员。没有人能完全拥有或控制因特网，因特网是一个不属于任何一个组织或个人的开放网络，只要是遵照协议 TCP/IP 的主机，均可上网。因特网代表着全球范围内一组无限增长的信息资源，其内容之丰富是任何语言都难以描述的。它是第一个实用的信息网络，入网用户既可以是信息的消费者，也可以是信息的提供者。随着一个又一个的计算机接入，因特网的实用价值愈来愈高，因此因特网早期以科研教育为主的运营性质正在被突破，应用领域越来越广，除商业领域外，政府上网也日益普及，借助因特网的电子政务发展得也很快。

一般来说，因特网可以提供以下主要服务。

（1）万维网（WWW）服务：可以通过 WWW 服务进行浏览新闻，下载软件，购买商品，收听音



乐，观看电影，网上聊天，在线学习，等等。

（2）电子邮件（E-mail）服务：可以通过因特网上的电子邮件服务器发送和接收电子邮件，进行信息传输。

（3）搜索引擎服务：可以帮助用户快速查找所需要的资料、想访问的网站、想下载的软件或者是所需要的商品。

（4）文件传输（FTP）服务：提供了一种实时的文件传输环境，可以通过 FTP 服务连接远程主机，进行文件的下载和上传。

（5）电子公告板（BBS）服务：提供一个在网上发布各种信息的场所，也是一种交互式的实时应用。除发布信息外，BBS 还提供了类似新闻组、收发电子邮件、聊天等功能。

（6）远程登录（Telnet）服务：可以通过远程登录程序进入远程的计算机系统。只要拥有在因特网上某台计算机的账号，无论在哪里，都可以通过远程登录来使用该台计算机，就像使用本地计算机一样。

（7）新闻组（UseNet）服务：这是为需要进行专题研究与讨论的使用者开辟的服务，通过新闻组既可以发表自己的意见，也可以领略别人的见解。

2.1.2 我国的因特网

中国是第 71 个加入因特网的国家级网络，1994 年 5 月，以“中科院—北大—清华”为核心的“中国国家计算机网络设施”（NCFC，The National Computing and Network Facility Of China，也称中关村网）与因特网联通。随后，我国陆续建造了基于 TCP/IP 技术的并可以和因特网互联的 4 个全国范围的公用计算机网络，它们分别是：中国公用计算机互联网 CHINANET，中国金桥信息网 CHINAGBN，中国教育科研计算机网 CERNET，以及中国科技网 CSTNET，其中前两个是经营性网络，而后两个是公益性网络。最近两年又陆续建成了中国联通互联网、中国网通公用互联网、宽带中国、中国国际经济贸易互联网、中国移动互联网等。

CHINANET 始建于 1995 年，由中国电信负责运营，是上述网络中最大的一个，是我国最主要的因特网骨干网。它通过国际出口接入因特网，从而使 CHINANET 成为因特网的一部分。CHINANET 具有灵活的接入方式和遍布全国的接入点，可以方便用户接入因特网，享用因特网上的丰富资源和各种服务。CHINANET 由核心层、接入层和网管中心 3 部分组成。核心层主要提供国内高速中继通道和连接“接入层”，同时负责与因特网的互联，核心层构成 CHINANET 骨干网。接入层主要负责提供用户端口以及各种资源服务器。

2003 年底，中国互联网络信息中心（CNNIC，China Network Information Center）公布：我国上网计算机数约 3089 万台，我国上网用户人数约 7950 万人，CN 下域名数量为 340 040 个，WWW 站点为 595 550 个。经营性骨干网有：中国电信集团公司、中国联通公司、中国网通公司、中国吉通公司、中国移动通信公司、中国通信广播卫星公司，中国有 4 只 .com 网络概念股在

NASDAQ 上市，分别是新浪、搜狐、网易、中华网。

我国国际出口带宽的总容量为 27 216Mbps，连接的国家有美国、加拿大、澳大利亚、英国、德国、法国、日本、韩国等，具体分布情况如下：

- 中国科技网（CSTNET）：155Mbps。
- 中国公用计算机互联网（CHINANET）：16 500Mbps。
- 中国教育和科研计算机网（CERNET）：447Mbps。
- 中国联通互联网（UNINET）：1490Mbps。
- 中国网通公用互联网（网通控股）（CNCNET）：3592Mbps。
- 宽带中国 CHINA169 网（网通集团）：4475Mbps。
- 中国国际经济贸易互联网（CIETNET）：2Mbps。
- 中国移动互联网（CMNET）：555Mbps。

2.1.3 接入因特网的方法

如果用户想使用因特网提供的服务，首先必须将自己的计算机接入因特网，然后才能访问因特网中提供的各类服务与信息资源。

1. 通过公共交换电话网（PSTN，Public Switched Telephone Network）接入因特网

所谓通过公共交换电话网接入因特网，是指用户计算机使用调制解调器通过普通电话与因特网服务提供商（ISP，Internet Service Provider）相连接，再通过 ISP 接入因特网。图 2-1 显示了通过 PSTN 接入因特网的结构。

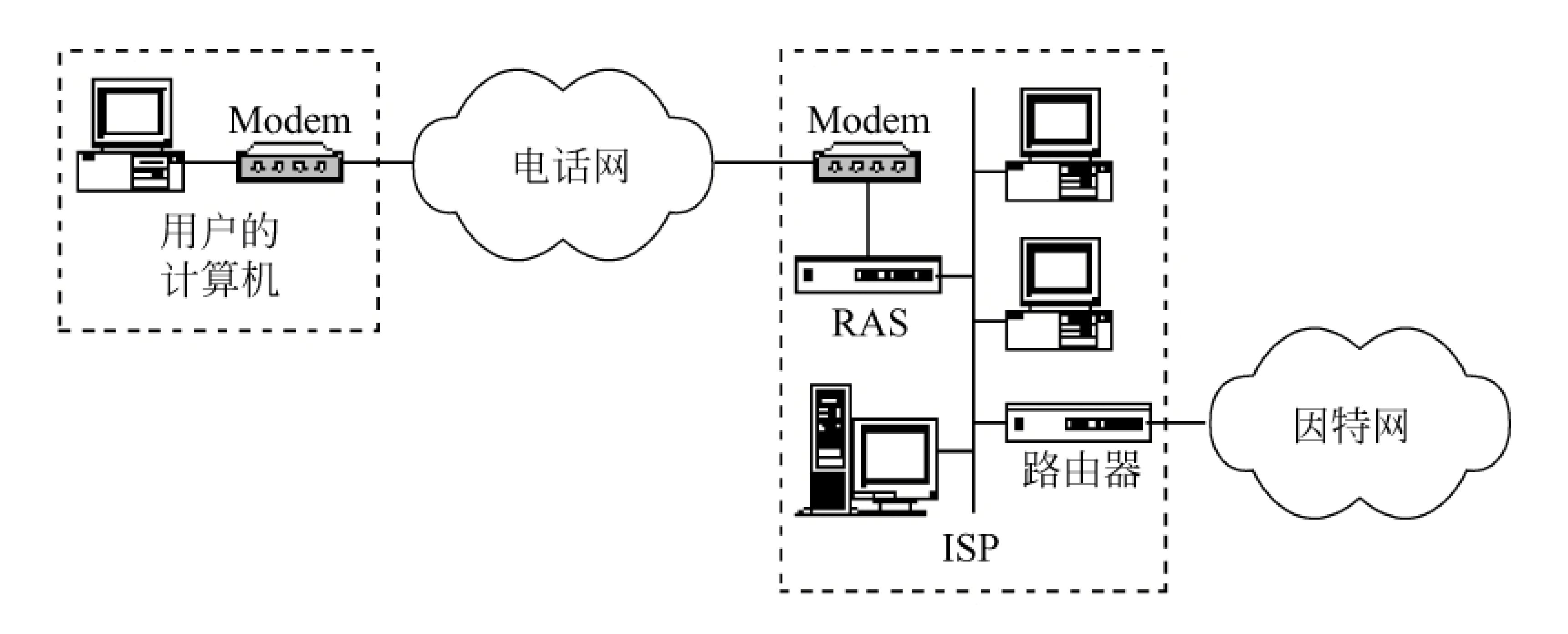
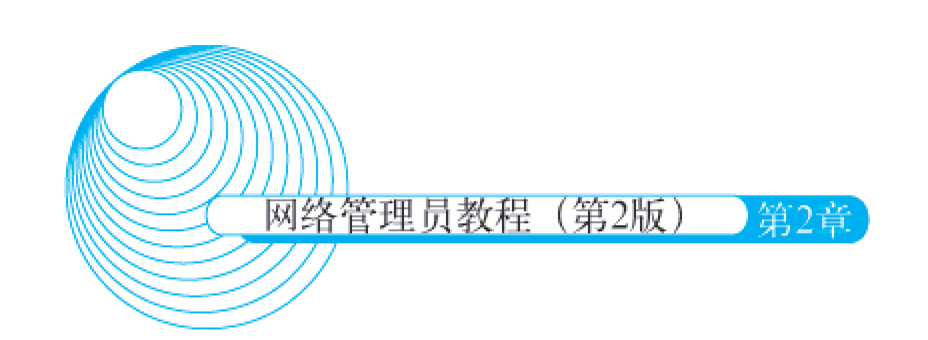


图 2-1 通过 PSTN 接入因特网

用户的计算机与 ISP 的远程接入服务器（RAS，Remote Access Server）均通过调制解调器与电话网相连。用户在访问因特网时，通过拨号方式与 ISP 的 RAS 建立连接，通过 ISP 的路由器访问因特网。在用户端，既可以将一台计算机直接通过调制解调器与电话网相连，也可以利用



代理服务器将一个局域网间接通过调制解调器与电话网相连。由于电话线支持的传输速率有限，目前较好线路的最高传输速率可以达到50kbps左右，一般线路只能达到30～40kbps，而较差线路的传输速率会更低。因此，这种方式只适合于个人或小型企业使用。

电话拨号线路除受速率的限制外，另一个特点就是需要通过拨号建立连接，由于技术本身的原因，在大量信息的传输过程中，连接有时会断开。

2. 通过综合业务数字网(ISDN，Integrated Services Digital Network)接入因特网

近年来，ISDN线路在国内发展十分迅速，通过它上网也不失为一种好的选择。这里指的是采用了基本速率接口(BRI，Basic Rate Interface)2B＋D的N-ISDN，在各用户终端之间实现以64kbps速率为基础的端到端的透明传输，上网传输速率最高可达128kbps，提供端到端的数字连接，用来承载包括话音和非话音在内的各种通信业务，可同时支持上网、打电话、传真等多种业务，俗称一线通。

就目前来说，ISDN最大的市场是上网。普通电话线上网的速率大多为40kbps左右，最多也不过56kbps，而ISDN为64kbps，最大可到128kbps；模拟电话线只能传送模拟话音信号，只能提供单一的电话业务。而ISDN实现了用户线的数字化，可同时支持多种业务。ISDN可同时接入多个设备，但不能像模拟电话一样把电话机直接接到电话线上，而需先接入一个被称为网络终端(NT，Network Terminal)的设备(该设备是局端设备，一般由电信局提供)，再接入电话机、传真机以及上网用的适配卡等。

非ISDN标准终端、普通话机可以通过终端适配器(TA，Terminal Adapter)、网络终端接入ISDN网络。标准ISDN终端、数字话机或G4传真机等其他标准ISDN用户终端设备通过网络终端接入ISDN网络。图2-2是各种终端接入ISDN网络的示意图。

3. 通过非对称数字用户环路(ADSL)接入因特网

ADSL(Asymmetric Digital Subscriber Line，非对称数字用户线)是xDSL家族中的一员。DSL(Digital Subscriber Line，数字用户环路)是以普通铜质电话线为传输介质的系列传输技术，它包括普通DSL、HDSL(对称DSL)、ADSL(不对称DSL)、VDSL(甚高比特率DSL)、SDSL(单线制DSL)、CDSL(Consumer DSL)等。

ADSL调制解调技术的主要特点在于：ADSL技术利用现有电话铜线为基础，几乎能为所有家庭和企业提供各种服务，用户能以比普通Modem高100多倍的速率通过数据网络或因特网进行交互式通信或取得其他相关服务。在这种交互式通信中，ADSL的下行线路可提供比上行线路更高的带宽，即上下行带宽不相等，且一般都在1∶10左右。如果线路的上行速率是640kbps，则下行线路就有6.4Mbps的高速传输速率。这也就是ADSL为什么叫非对称数字用户环路的原因，其非对称性特点尤其适合于开展上网业务。同时，ADSL采用频分复用技术，可

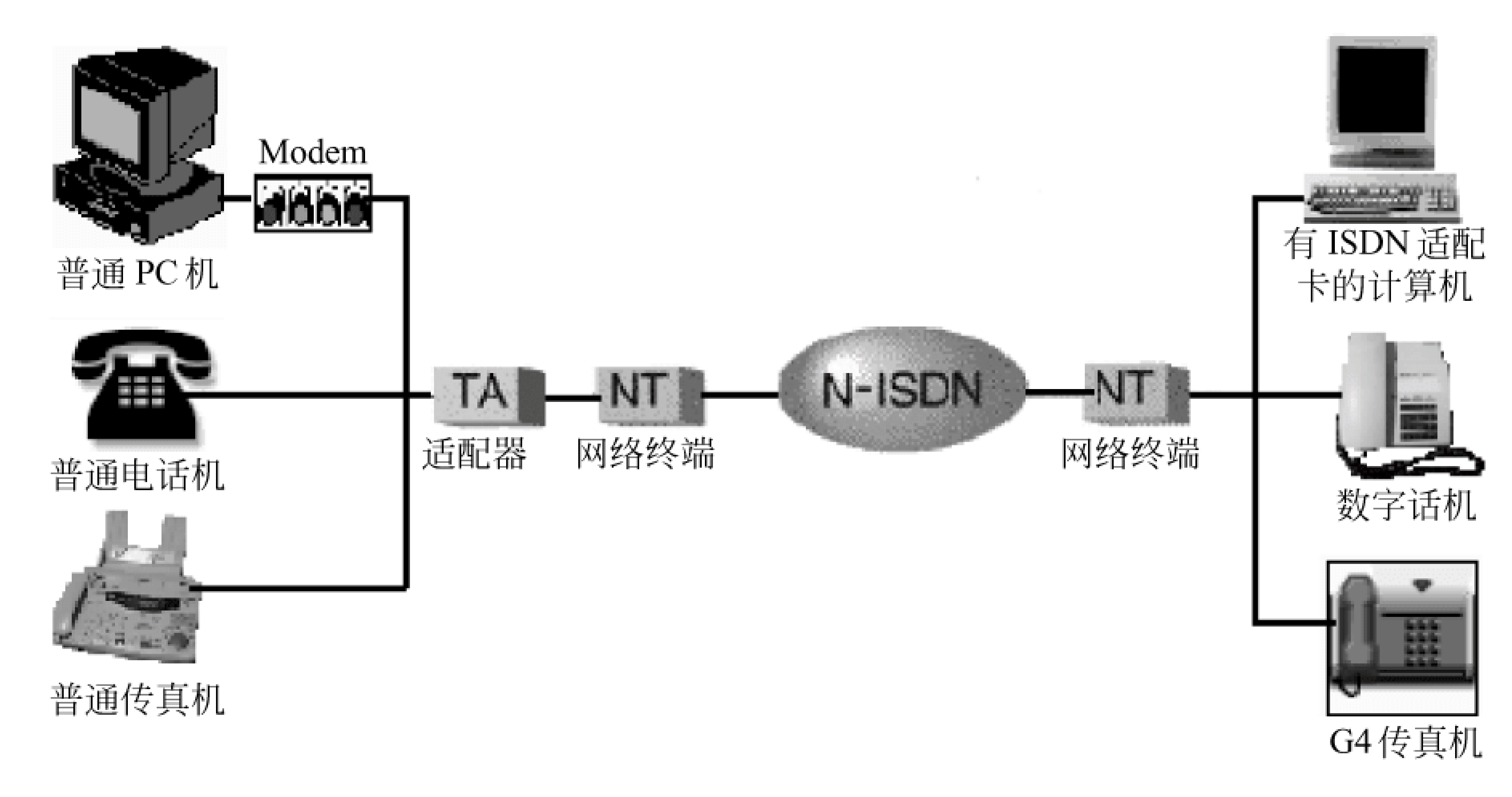


图 2-2　各种终端接入 ISDN 网络的示意

将电话语音和数据流一起传输，用户只须加装一个 ADSL 用户端设备，通过分流器（话音与数据分离器）与电话并联，便可在一条普通电话线上同时通话和上网且互不干扰。因此，使用了 ADSL 接入方式，等于在不改变原有通话方式的情况下，另外增加了一条高速上网专线。可见，ADSL 技术与拨号上网调制技术有很大的区别。

调制技术是 ADSL 的关键所在。在 ADSL 调制技术中，一般均使用高速数字信号处理技术和性能更佳的传输码型，用以获得传输中的高速率和远距离。ADSL 能够在现有的铜线环路，即普通电话线上提供最高达 8Mbps 的下行速率和 640kbps 的上行速率，传输距离达 3～5km，是目前几种主要的宽带网络接入方式之一。其优势在于可以充分利用现有的电话线网络，在线路两端加装 ADSL 设备即可为用户提供高带宽服务。由于不需要重新布线，所以降低了成本，进而减少了用户上网的费用。

ADSL 的接入方式主要有两种：

（1）专线入网方式：用户拥有固定的静态 IP 地址，24 小时在线。

（2）虚拟拨号入网方式：并非是真正的电话拨号，而是用户输入账号、密码，通过身份验证，获得一个动态的 IP 地址，可以掌握上网的主动性。

ADSL 的接入模型主要由中央交换局端模块和远端模块组成，如图 2-3 所示。

中央交换局端模块包括在中心位置的 ADSL Modem 和接入多路复合系统（DSLAM，DSL Access Multiplexer），处于中心位置的 ADSL Modem 被称为 ATU－C（ADSL Transmission Unit－Central）。

远端模块由用户 ADSL Modem 和滤波器组成，用户端 ADSL Modem 通常被称为

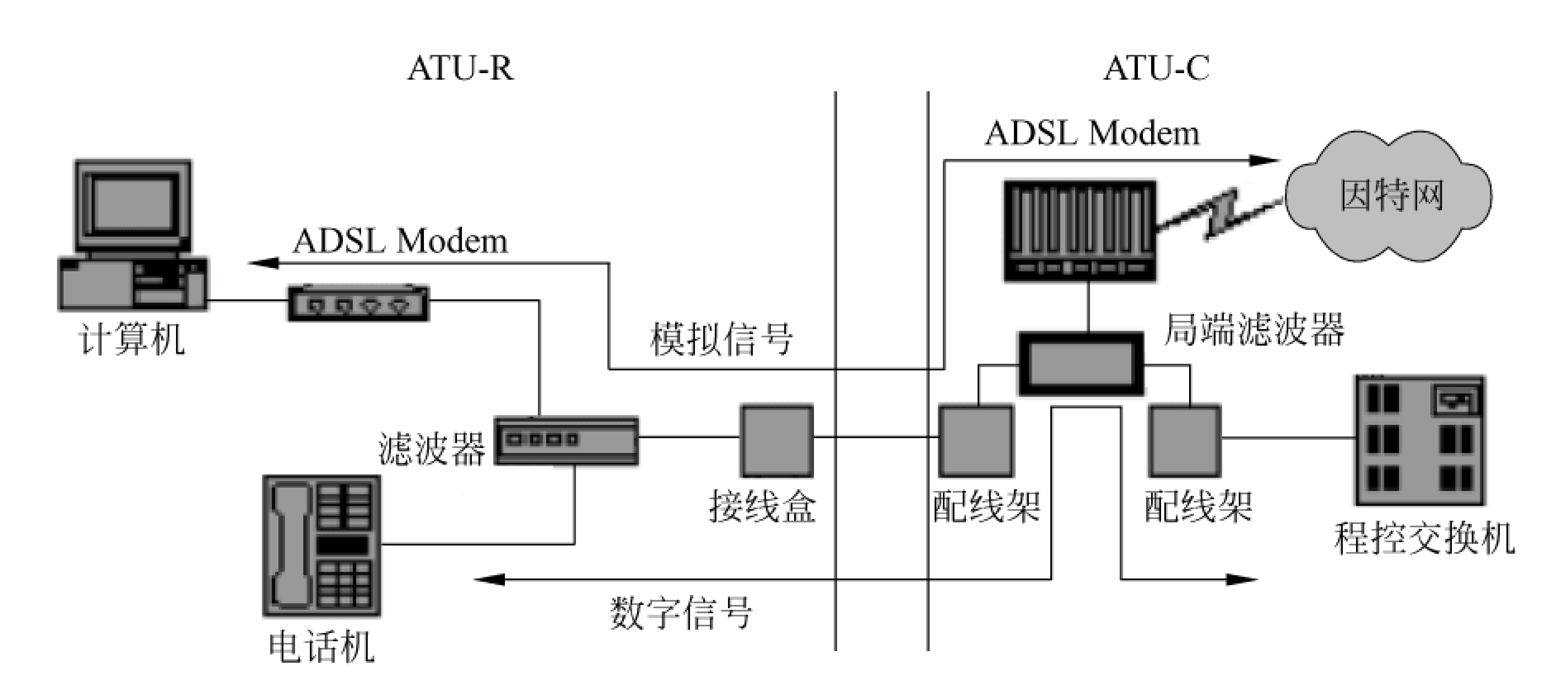


图 2-3　通过 ADSL 接入因特网

ATU－R(ADSL Transmission Unit－Remote)。

ADSL 安装包括局端线路调整和用户端设备安装两部分。在局端方面，由 ISP 在用户原有的电话线中串接 ADSL 局端设备；用户端的 ADSL 安装也非常简易方便，只要将电话线连上滤波器，滤波器与 ADSL Modem 之间用一条两芯电话线连上，ADSL Modem 与计算机的网卡之间用一条交叉网线连通即可完成硬件安装，再将 TCP/IP 协议中的 IP、DNS 和网关参数项设置好，便完成了安装工作。

4. 通过局域网接入因特网

所谓“通过局域网接入因特网”，是指用户通过局域网，局域网使用路由器通过数据通信网与 ISP 相连接，再通过 ISP 接入因特网。图 2-4 显示了通过局域网接入因特网的结构。

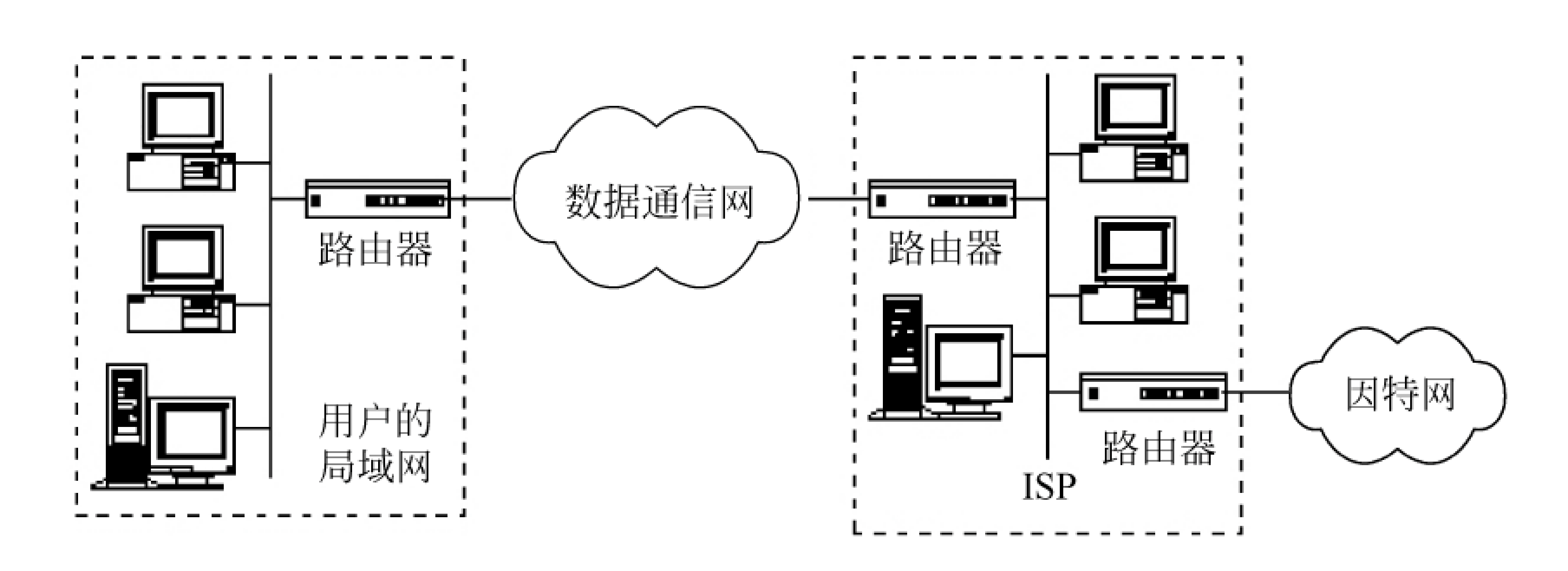


图 2-4　通过局域网接入因特网

数据通信网有很多种类型，例如 DDN、ISDN、X.25、帧中继与 ATM 网等，它们均由电信部门运营与管理。目前，国内数据通信网的经营者主要有中国电信与中国联通。采用这种接入方

式时，用户花费在租用线路上的费用比较昂贵，用户端通常是有一定规模的局域网，例如一个企业网或校园网。

2.2 WWW 基本应用

2.2.1 WWW 的概念

1. 什么是 WWW

WWW(World Wide Web)，称为万维网或称全球信息网，WWW 又简称 3W 或 Web，是集文字、图像、声音和影像为一体的超媒体。Web 的英文本意是蜘蛛网，之所以将其引申为全球信息网，就是因为全球信息网正是由这些像千丝万缕的蜘蛛网一样的超链接连接在一起的。WWW 是目前因特网上最为先进、交互性能最好、应用最为广泛的信息检索工具，它为用户提供了一个可以轻松驾驭的图形化用户界面，以方便查阅因特网上的文档，这些文档与它们之间的链接一起构成了一个庞大的信息网。

Web 允许通过“超链接”从某一页跳到其他页，如图 2-5 所示。可以把 Web 看成一个巨大的图书馆，Web 节点就像一本书，而 Web 页好比书中特定的页，页可以包含文档、图像、动画、声音、3D 世界以及其他任何信息，而且能够存放在全球任何地方的计算机上。Web 融入了大量的信息，从商品报价到就业机会、从电子公告牌到新闻、电影预告、文学评论以及娱乐等。多个 Web 页合在一起便组成了一个 Web 节点。用户可以从一个特定的 Web 节点开始 Web 环游之旅。人们常常谈论的 Web“冲浪”就是访问这些节点，“冲浪”意味着沿超链接转到那些相关的 Web 页和专题，可以会见新朋友、参观新地方以及学习新的东西。用户一旦与 Web 连接，就可以使用相同的方式访问全球任何地方的信息，而不用支付额外的“长距离”连接费用或受其他条件的制约。Web 正在逐步改变全球用户的通信方式，这种新的大众传媒比以往的任何一种通讯媒体都要快捷，因而受到人们的普遍欢迎。

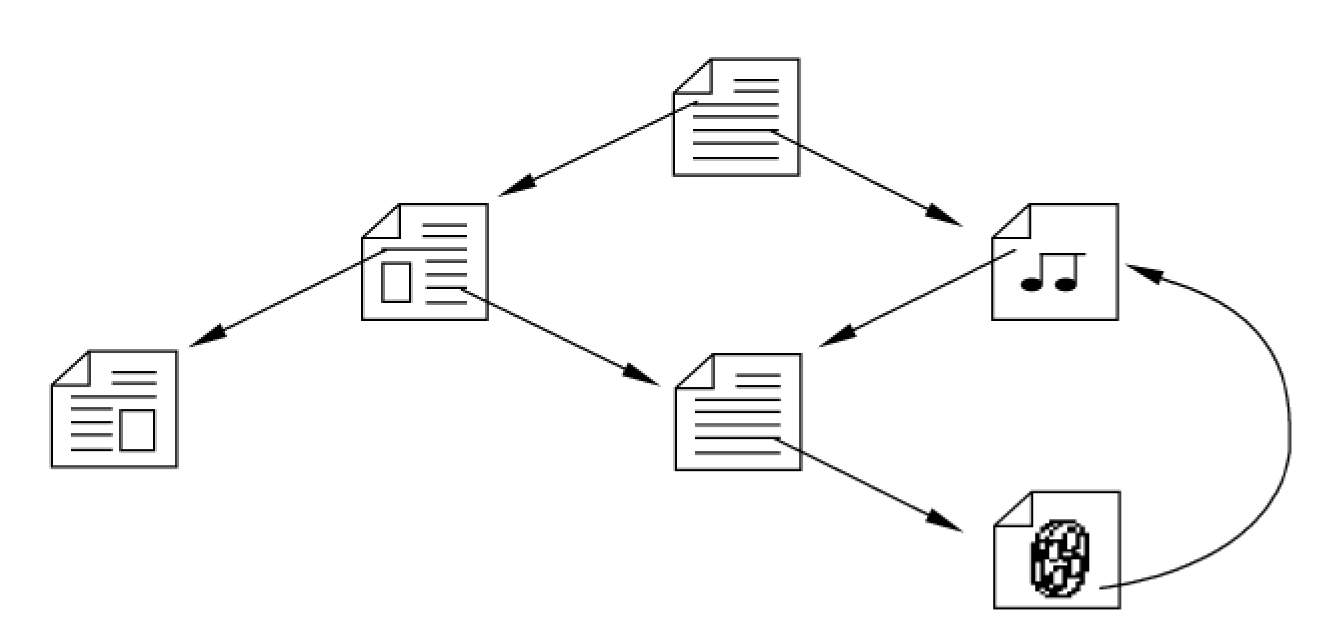
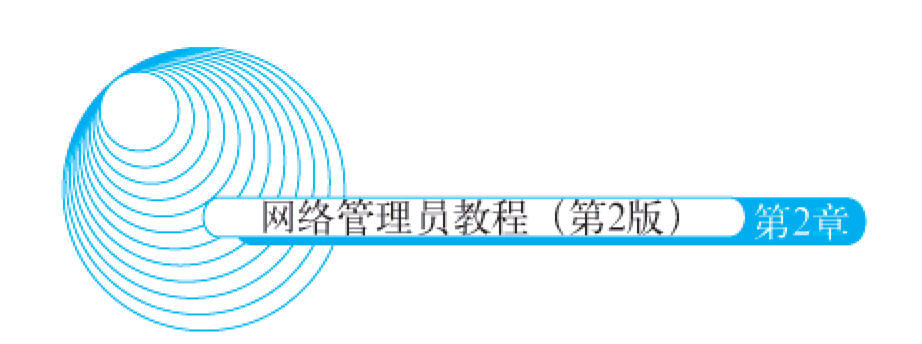


图 2-5　WWW 超链接示意



2. 超文本(Hypertext)

学习 WWW 还要了解超文本与超媒体的基本概念,因为它们是 WWW 的信息组织形式,也是 WWW 实现的关键技术之一。所谓超文本,就是含有超链接的文本。

长期以来,人们一直在研究如何对信息进行组织,其中最常见的组织方式就是按书籍的目录结构。书籍目录采用有序的方式来组织信息,它将所要描述的信息内容按照章、节的分级结构组织起来,读者可以按照章、节的顺序阅读。随着计算机技术的发展,人们不断推出新的信息组织方式,以方便对各种信息的访问。在 WWW 系统中,信息是按超文本方式组织的。用户在浏览文本信息的同时,随时可以选中其中的超链接,进一步到指定位置访问相关信息。超链接往往是上下文的关联词,通过选择超链接可以跳转到其他文本信息。

3. 超媒体(Hypermedia)

超媒体进一步扩展了超文本所链接的信息类型,用户不仅能从一个文本跳到另一个文本,而且可以激活一段声音,显示一个图形,甚至是播放一段动画。目前流行的多媒体电子书籍大都采用这种方式。例如,在一本多媒体儿童读物中,当读者选中屏幕上显示的老虎图片、文字时,可以同时播放一段关于老虎的动画。超媒体可以通过这种集成化的方式,将多种媒体的信息通过超链接联系在一起。

4. 主页(Homepage)

主页,英文是 Homepage,直译为首页。主页,又叫网页,有时也称 Web 页。主页用于 WWW 服务进行信息的查询和浏览,文档扩展名为.html 或.htm。“主页”是某一个 Web 节点的起始点,它就像一本书的封面或者目录,是个人或机构的基本信息页面。用户通过主页可以访问有关的信息资源。在 WWW 环境中,信息是以主页的形式出现的,这些主页是以超文本和超媒体格式编写的。通常将编写主页的语言称为 HTML(Hypertext Markup Language),即超文本标记语言,这是一种计算机描述语言,专门用来编写 Web 页。

主页一般包含以下几种基本元素。

(1) 文本(Text):是最基本的元素,就是通常所说的文字。

(2) 图片(Image):主页中最常见的两种图像格式是 GIF 与 JPEG。

(3) 表格(Table):类似于 Word 中的表格,在主页中插入表格,更加有利于页面的整齐与规范。

(4) 超链接(Hyperlink):HTML 中的重要元素,用于将 HTML 元素与其他主页相连。

5. URL 与信息定位

在因特网中有如此众多的服务器,而每台服务器中又包含很多共享信息,如何找到需要的

信息呢？在访问因特网的客户机上，“浏览器”是用于查看 Web 页的软件工具。“浏览器”在访问因特网中服务器的共享信息时，需要使用统一资源定位器（URL，Uniform Resource Locator）。用户可以通过使用 URL，指定要访问哪种类型的服务器，哪台服务器，以及哪个文件。如果用户希望访问某台 WWW 服务器中的某个页面，只要在浏览器中输入该页面的 URL 地址，就可以方便地浏览到该页面。

标准的 URL 由 3 部分组成：服务器类型、主机名和路径及文件名。例如：

- 清华大学 WWW 服务器的 URL 地址为 http://www.tsinghua.edu.cn。
- 清华大学 FTP 服务器的 URL 地址为 ftp://ftp.tsinghua.edu.cn。

其中，http 和 ftp 指出的是服务器类型，在这里是用访问这台服务器要使用的协议来代替的。http 是超文本传输协议，ftp 是文件传输协议。www.tsinghua.edu.cn 和 ftp.tsinghua.edu.cn 指出的是要访问的服务器的主机名，也就是一个域名地址。

通常，在 URL 中省略路径及文件名，当然在实际应用中也可以采用路径及文件名，例如：http://go5.162.com/～garyzgm/index.html。

6. 浏览器

前面提到，浏览 WWW 站点需要浏览器，那么，什么是浏览器呢？WWW 浏览器是用来浏览因特网主页的工具软件。WWW 浏览器的功能非常强大，利用它可以方便地访问因特网上的各类信息，目前版本的浏览器基本上都支持多媒体，可以通过浏览器来播放声音、动画与视频，使得 WWW 世界变得更加丰富多彩。现在人们使用最多的浏览器软件是 Netscape 公司的 Communicator 和 Microsoft 公司的 Internet Explorer。

Internet Explorer 是由美国 Microsoft 公司开发的 WWW 浏览器软件，它的中文意思是“因特网探索者”，通常人们把它叫做 IE，可以使用 IE 来浏览主页，下载文件，收发电子邮件，阅读新闻组，制作与发表主页等。如果说因特网是大海，那么 Explorer 就是轮船，就是这艘轮船的舵手。IE 的出现虽比 Navigator 晚一些，但由于 Microsoft 公司的 Windows 在操作系统领域的优势，以及它本身是一个免费软件，所以它在浏览器市场的占有率逐年增长，IE 和 Windows 98、Windows 2000、Windows XP 都集成在一起，在安装操作系统的同时，IE 被自动安装。安装了浏览器以后，就可以访问主页了。

Communicator 的前一个版本是 Navigator，是 Netscape 公司开发的最为流行的浏览器软件之一，Navigator 虽然不是第一个浏览器，但却是第一个多媒体浏览器，正是由于它的出现才真正掀起了 WWW 的狂潮，可以说 Navigator 为今天因特网的迅速普及起到了极大的推动作用。

2.2.2 利用 IE 浏览 Web 网页

1. 浏览网页

例如要访问中央电视台的主页，首先连接网络，然后在 URL 地址栏里输入中央电视台的网址 www. cctv. com. cn，按 Enter 键即开始从 WWW 服务器下载 HTML 代码。代码接收完毕时，状态栏会显示“完成”，浏览器开始解释执行这些下载的代码，解释执行的结果就是主页。如图 2-6 所示。



图 2-6 中央电视台网站 2004 年 3 月 6 日的主页

在浏览主页的时候，鼠标的指针形状在超链接所在位置，会由箭头变成手指☝，凡是能变成手指的地方，单击鼠标左键，就会出现相应的新页面，这就是超链接的跳转，通过超链接的跳转可以轻松直观地获取所希望的信息，并且不断深入地挖掘所感兴趣的内容。

在浏览网页时如果看到想要的资料，可用鼠标选定相应内容，通过“编辑”菜单下的“复制”命令，将相应内容复制到剪贴板上，再在其他应用程序中将其“粘贴”过来，从而达到信息的共享。当然，也可以单击工具栏上的“打印”按钮，将感兴趣的页面打印出来。

2．保存网页

在浏览网页时，如果阅读比较长的文章，可先将其保存到本地硬盘，然后再离线浏览，这样可以大量节省上网费用。另外，如果遇到具有保留价值的信息，或者是想引用的信息，都需要保存到本地硬盘。

保存网页的具体方法是，待欲保存网页下载完成后，选择“文件”菜单下的“另存为”菜单，在弹出的保存 Web 页对话框中，选择该文件要保存的位置，并指定一个文件名，然后单击“保存”按钮，如图 2-7 所示。保存完成后，可在保存该文件的文件夹中，找到并双击该文件，该文件会在 IE 中打开，此时即为离线浏览。



图 2-7　保存 Web 页

3．保存图片

在进行网页浏览时，经常会看到一些精美的图片，或有保留价值的图片，如果要将网页中的某张图片作为资料保存在硬盘中，具体操作方法如下：

将鼠标移动到该图片上，单击鼠标右键，然后在弹出的快捷菜单中选择“图片另存为”选项，如图 2-8 所示。这时将会弹出“保存图片”对话框，在弹出的对话框中，选择该图片保存的位置和类型，并为其指定一个文件名，然后单击“保存”按钮即可。

2.2.3　WWW 搜索引擎

上网不仅仅是收发电子邮件、阅读新闻，还应学会查询资料，虽然因特网中的知识包罗万

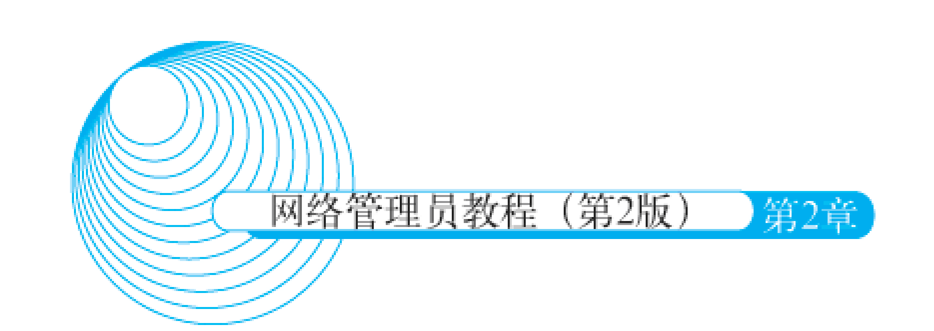




图 2-8 保存图片操作

象，但如果需要查找特定的专业信息，还是需要费一番周折的，这时，通常都需要通过搜索引擎来实现，常见的中文搜索引擎有：Google（www.google.com）、百度（www.baidu.com 或 d.baidu.com）、搜狐（www.sohu.com）和新浪（www.sina.com.cn）等。在搜索引擎中可以搜索的内容包括网页、MP3、图片、Flash、新闻、软件等诸多信息。

1. 搜索方法

在进行搜索之前要做好以下 3 项准备工作。

（1）选定搜索引擎，选定搜索功能，了解所选搜索引擎的搜索方法。

（2）确定搜索概念或意图。选择描述这些概念的关键字及其同义词或近义词等。

（3）建立搜索表达式，使用符合该搜索引擎语法的正确表达式，开始搜索。

下面以百度中文搜索引擎为例，查找有关动态网页制作技术的有关资料。在搜索栏的关键词位置输入“动态网页制作技术”，然后单击“百度搜索”按钮，如图 2-9 所示。

很快，就会看到在窗口中出现的搜索结果，如图 2-10 所示，百度中文搜索引擎找到 843 个包

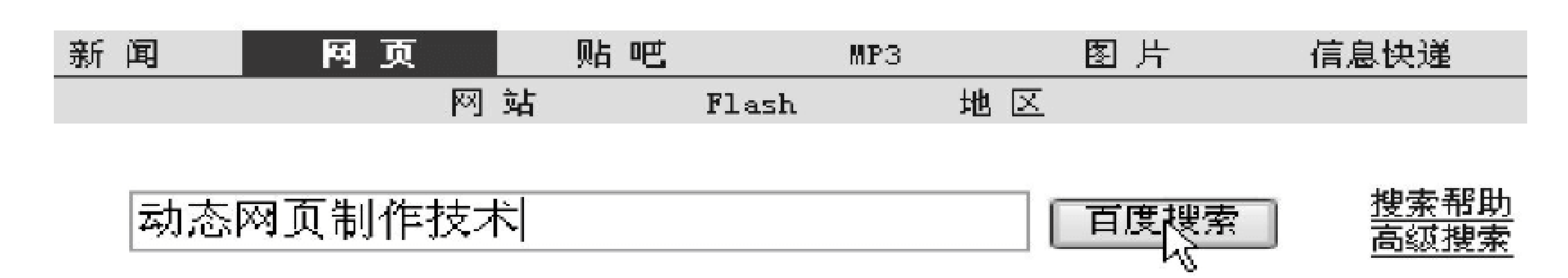


图 2-9　输入搜索关键字

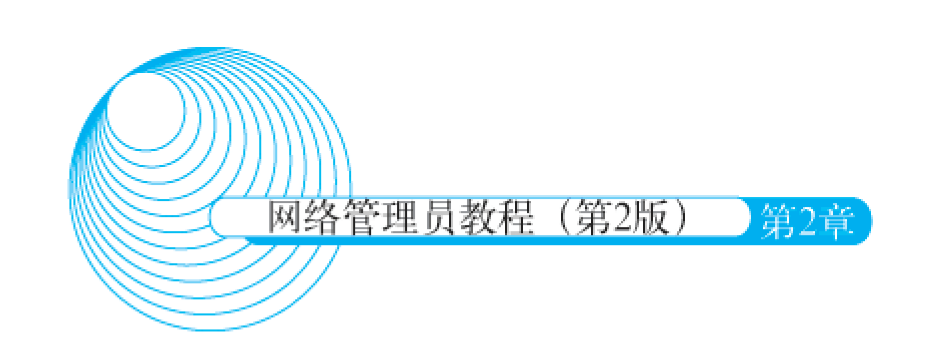
含“动态网页制作技术”内容的网页。



图 2-10　搜索结果

在搜索结果中查看页面或网站的简介时，如有必要，单击相应的超链接，进入相关的网页。有时候搜索结果并不理想，内容不集中，此时可进一步进行搜索。比如，想在搜索结果中进一步搜索包含“ASP”内容的网页，则在搜索栏中输入“ASP”，然后单击“在结果中找”按钮，如图 2-11 所示。

稍后，就会看到在窗口中出现的进一步的搜索结果，如图 2-12 所示。找到 588 个符合包含“动态网页制作技术”和“ASP”内容的网页。



搜索技巧 免费搜索代码 高级搜索

ASP 百度搜索 在结果中找

图 2-11　输入进一步搜索关键字



图 2-12　进一步搜索结果

2. 搜索技巧

（1）如果返回的结果是“没有找到匹配的网页”、“返回 0 个页面”。这时通常要检查一下关键字中有没有错别字或语法错误，或换用不同的关键词重新搜索。也可能是有的搜索表达式所设定的范围太窄了，建议将原关键词拆成几个关键词来搜索，词与词之间用空格隔开。

例如，搜索“动态　网页制作技术”，可以找到 6140 篇资料。而搜索“动态网页制作技术”，则只有严格含有“动态网页制作技术”连续 7 个字的网页才能被找出来。前者的搜索范围较为宽松，后者的搜索范围则比较严格。

（2）如果返回的结果极多，成千上万，而且许多结果与需要的主题无关。这时通常需要排除

含有某些词语的资料以利于缩小查询范围。

百度支持“—”功能，用于有目的地删除某些无关网页，但减号之前必须留有空格，语法是“A —B”。例如，要搜寻关于“动态网页制作技术”，但不含“JSP”的资料，可使用“动态网页制作技术 —JSP”作关键字进行查询。

(3) 如果希望更准确地利用百度进行搜索，却又不熟悉繁杂的搜索语法，在高级搜索功能中可以自己定义要搜索的网页的时间、地区、语言、关键词出现的位置，以及关键词之间的逻辑关系等。高级搜索功能使百度搜索引擎功能更完善，信息检索也更加准确、快捷。

3. 评估网上信息

网上的信息很多，但并非所有的信息都有使用价值。因为任何人、任何单位都可能在网上发布信息，所以，这些信息中就有相当一部分是所谓的“垃圾信息”。所以通过因特网获取信息时，不得不鉴别哪些信息是有用的、值得信赖的，哪些信息应该选择性地接受，哪些信息应该彻底抛弃。

下面简单地说明一下评估网上信息的基本技巧。

(1) 从页面上部或底部寻找作者姓名、组织机构名称或公司名称，如果是个人页面，那么是否有作者的简介，看看他的受教育程度、职位、所属单位等；如果是一个组织机构或公司，则看是否有详细的介绍页面，其历史怎样？发布这些信息的目的如何？这些个人或单位是否听说过？是否是所熟悉的？信誉是否良好？这些都有助于判读其页面内容的可信程度。

比如：赛迪网，从它的主页上很容易找到“关于本站”这个按钮，里面有赛迪网的简介、相关编辑及联系方式。如果对哪个内容有疑问，可以直接发电子邮件或打电话与编辑联系。赛迪网操作方式上的正规性可以从各个细小的方面体现出来。如此正规的网站，其内容的可信度肯定会比较大。

(2) 从 URL 上可以得到一些该网站的线索。比如：凡带有“～”符号的大都是个人主页。从域名的后缀上也可以得到一些大概的线索：

① .gov 或 .gov.cn 是政府网站，一般比较权威、可靠，不会随意发布不准确的信息。

② .edu 是教育类网站，既可能是严肃的学术研究，也可能是学生随意制作的主页。

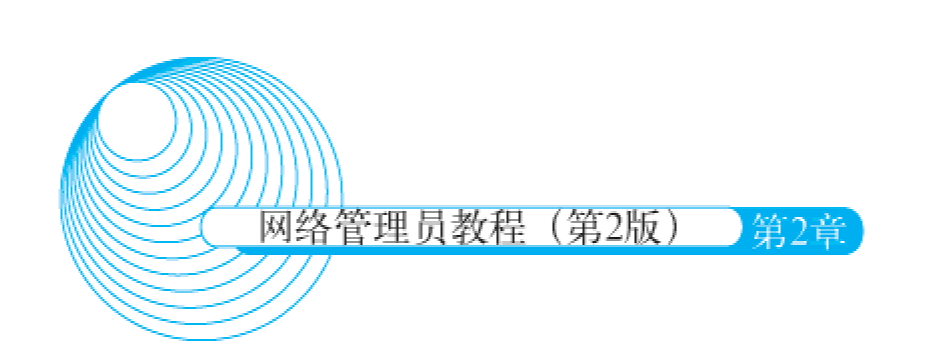
③ .com 或 .com.cn 是商业网站，最常见。在介绍产品时往往会夸大其辞，所以要注意选择性地接受。

④ .net 是网络服务公司，为商业或个人用户提供服务。

⑤ .org 一般是非赢利性组织，其观点可能带有倾向性。

(3) 访问该站点的主页，查看一下该组织的相关资料。如果页面上没有去主页的链接，可以直接访问 URL 前部的地址，那往往就是该网站的首页。

如：http://www.yesky.com/staticpages/builder/builder_schedule/asp.html 这一大串网址，



把 URL 地址中/staticpages 以后的所有字母都删去，只留下 http://www.yesky.com，然后按 Enter 键，通常就能看到该网站的首页。

（4）利用搜索引擎查一下关于该组织或个人的其他资料。

（5）从页面顶部或底部查看该网页的最近更新日期。如果找不到的话，在 IE 工作窗口中右击选择“属性”，或者在顶部菜单中选择“文件”下面的“属性”，即可看到该网页的最近更新日期。

2.2.4 利用 WWW 服务下载文件

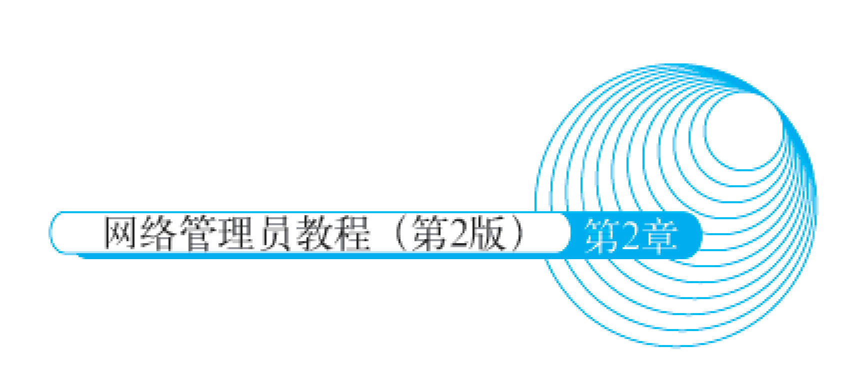
使用浏览器在浏览网页时可以通过相应的超链接进行文件的下载，很多 WWW 站点提供了大量的共享软件以供下载，这也是因特网吸引人的一个重要特点，国内也有很多专业的下载中心网站，另外，“搜狐”、“新浪”、“网易”等综合性网站也提供常见软件下载的功能。下面以使用 IE 在“新浪”中下载文件为例，讲解通过浏览器下载文件的步骤。

（1）启动 IE，访问“新浪”（www.sina.com.cn）主页，如果想要下载 QQ2003 软件，在搜索框中输入 QQ2003，搜索类别选择“软件”，然后单击“搜索”按钮，系统会自动搜索要查找的软件，如图 2-13 所示。



图 2-13 搜索 QQ2003 软件

（2）返回搜索结果页面，在搜索结果页面中显示了搜索到的关于 QQ2003 的软件名称及简



单介绍，单击“QQ2003III 正式版”超链接，如图 2-14 所示。



图 2-14　搜索结果页面

(3) 这时会给出程序的进一步介绍，同时会给出下载地址超链接窗口，单击具体的下载地址，如图 2-15 所示。

(4) 在弹出的“文件下载”对话框，选择“保存”按钮，如图 2-16 所示。

(5) 在弹出的“另存为”对话框，指定下载文件保存的目录和文件名，然后单击“保存”按钮，如图 2-17 所示。

(6) 弹出下载状态对话框，如图 2-18 所示。显示了下载网址、估计剩余时间、下载目录、传输速度等状态信息，下载完成后，默认情况下系统会自动关闭该对话框。

2.2.5　设置 IE 的 WWW 浏览环境

1. 常规设置

选择 Internet 选项菜单后会出现“Internet 选项”对话框，在“Internet 选项”对话框的“常规”选项卡中，默认的起始页为 Microsoft 公司主页 http://home.microsoft.com/intl/cn/，可以将其



图 2-15 下载地址超链接窗口



图 2-16 文件下载对话框



图 2-17　文件下载另存为对话框



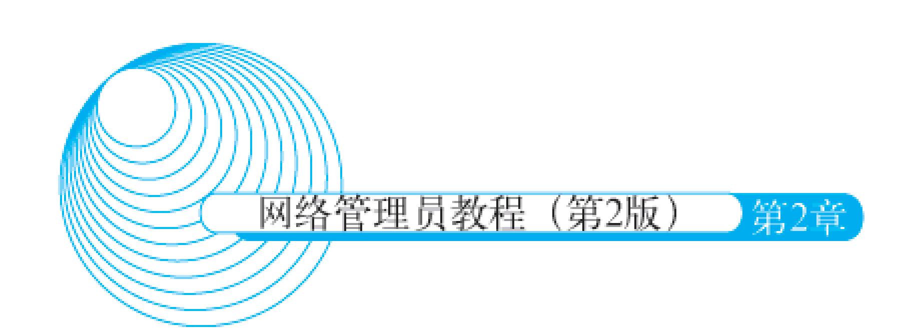
图 2-18　文件下载状态对话框

改成经常使用的“首都之窗”的主页 http://www.beijing.gov.cn，如图 2-19 所示。



图 2-19　“Internet 选项”的“常规”选项卡

浏览器会自动将访问过的主页保存到硬盘中的临时文件夹 C:\Windows\Temporary Internet Files 中，这样做的好处是，如果要访问的主页在临时文件夹中，访问的速度就会非常快。但也存在一个问题，也就是别人可以轻而易举地在这里找到曾经访问过的主页、下载的图片等信息。为了解决这一问题可以单击“常规”选项卡中的“删除文件”按钮，将临时文件夹中的信息



删除，单击“清除历史记录”则会删除所有访问过的网址记录。

2. 安全设置

在“Internet 选项”对话框的“安全”选项卡中，可以将 Web 站点分配到具有适当安全级的区域，如图 2-20 所示。

（1）Internet 区域：默认情况下，该区域包含了不在的计算机和 Intranet 上以及未分配到其他任何区域的所有站点。Internet 区域的默认安全级为“中”。

（2）本地 Intranet 区域：该区域通常包含按照系统管理员的定义不需要代理服务器的所有地址。本地 Intranet 区域的默认安全级为“中低”。

（3）可信站点区域：该区域包含信任的站点，相信可以直接从这里下载或运行文件，而不用担心会危害的计算机。可将站点分配到该区域。可信站点区域的默认安全级为“低”。

（4）受限站点区域：该区域包含不信任的站点，不能肯定是否可以从这里下载或运行文件而不损害的计算机，可将站点分配到该区域。受限站点区域的默认安全级为“高”。

3. 内容设置

在“Internet 选项”对话框中的“内容”选项卡中提供了分级审查功能，如图 2-21 所示。分级审查功能可以限制在本机访问那些受限制的站点，例如防止未成年人访问暴力色情站点。

在“Internet 选项”对话框的“内容”选项卡中，单击“启用”按钮，启动分级审查机制，如



图 2-20 “Internet 选项”的“安全”选项卡



图 2-21 “Internet 选项”的“内容”选项卡

图 2-22 所示。在“分级审查”的“分级”选项卡中可对“暴力”、“裸体”等类别进行级别设置，例如，选中“暴力”，并调节滑块到“级别 0：无暴力”。

需要说明的是，如果谁都可以操作设置分级审查功能，刚设置完，别人还可以改回来，那么分级设置就没有意义了。为此，还需要将“分级审查设置”这一功能加密，具体方法是，选择“分级审查”中“常规”选项卡，如图 2-23 所示。在“分级审查”的“常规”选项卡中，单击“更改密码”按钮，可设置监护人密码对分级审查设置功能进行保护。



图 2-22　Internet 选项的“分级审查”



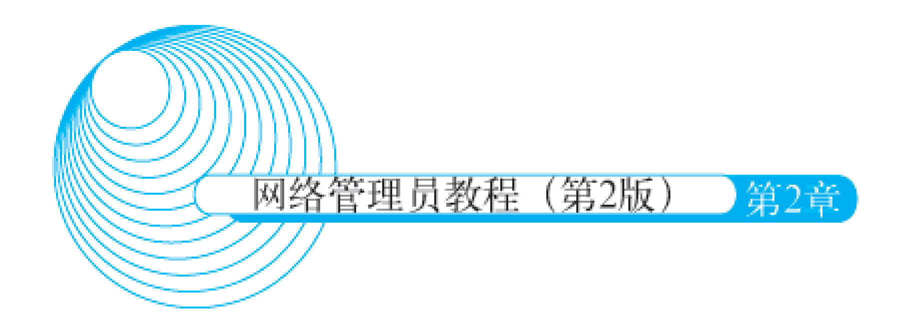
图 2-23　“分级审查”功能加密

4. 程序设置

在“Internet 选项”对话框的“程序”选项卡中，可以指定各种因特网服务使用的程序，如图 2-24 所示。例如系统默认的电子邮件程序是 Outlook Express，可以单击“电子邮件”下拉式列表框右边的下拉按钮，将其改为 Microsoft Outlook，这样，在使用 IE 发送电子邮件时，将自动打开 Microsoft Outlook 应用程序，而不是 Outlook Express。系统默认的 HTML 编辑器是 Microsoft FrontPage，可以单击下拉按钮，将其改为 Notepad，这样，在 HTML 文档上右击选择“编辑”命令时，或在浏览器的工具栏上单击“编辑”工具按钮时，将自动打开记事本应用程序编辑 HTML 文档，而不是 FrontPage。

5. 高级设置

在“Internet 选项”对话框的“高级”选项卡中，列出了超文本传输协议 HTTP、Java 虚拟机



Java VM、安全和多媒体等方面的设置。在“高级”选项卡中还提供了多媒体选项，如图 2-25 所示。对多媒体选项进行相应设置，可加快浏览或下载网页的速度。例如，只选中“显示图片”而不选中“播放动画”、“播放声音”、“播放视频”，甚至连“显示图片”都不选中，这样可以大大加快网页下载浏览的速度。




图 2-24 “Internet 选项”的“程序”选项卡

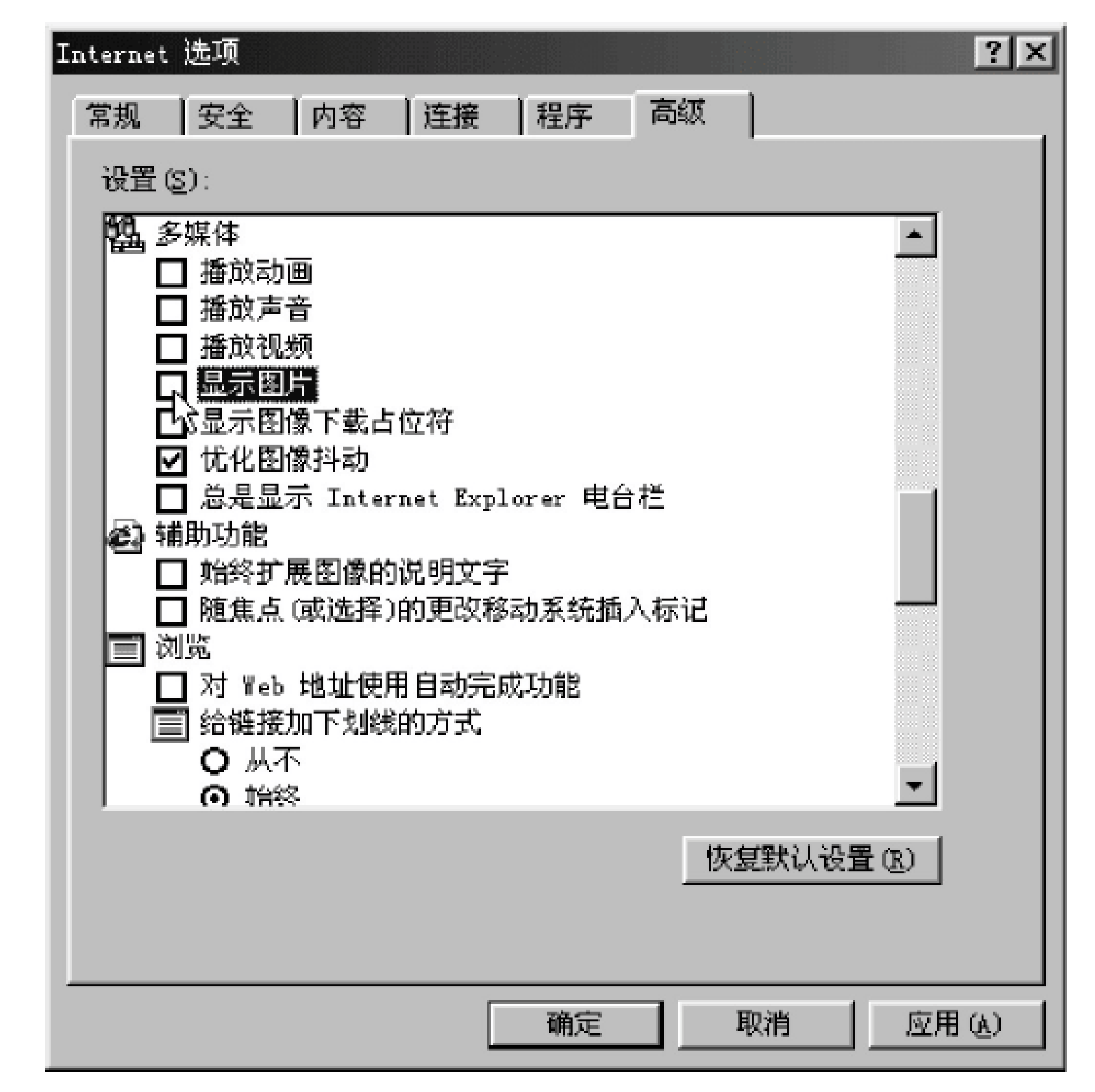


图 2-25 “Internet 选项”的“高级”选项卡

清除“显示图片”复选框后，如果当前页上的图片仍然可见，可选择“查看”菜单，然后单击“刷新”，以隐藏此图片。另外，即使清除了“显示图片”或者“播放视频”复选框，也可以通过鼠标右键单击相应图标，然后单击“显示图片”，在 Web 页上显示单幅图片或动画。

2.3 电子邮件

2.3.1 电子邮件系统的基本概念

2004 年 1 月第 13 次 CNNIC 的互联网络发展状况调查统计报告显示，网民人均拥有 1.4 个 E-mail 账号，其中免费的 E-mail 账号为 1.3 个。在最常用的因特网服务中，E-mail 的使用频率最高(88.4%)，这充分说明了 E-mail 的重要性。其他常用的因特网服务分别是搜索引擎、文件上传或下载服务、各类信息查询服务等，它们分别占到了：66.6%、50.56%、44.65%。目前，每天约有 2500 万人在各地发送电子邮件，尽管信件大多是文本形式，但现在实际上也可以传送图形、声音等二进制文件。

E-mail 是一种利用网络交换信息的非交互式服务。收发电子邮件的前提是，要拥有一个

属于自己的“邮箱”也就是 E-mail 账号。在办理上网手续时，可以向 ISP 申请，或者在因特网中申请一些免费的 E-mail 账号。有了账号也就有了邮箱地址，同时，还可以获得一个该邮箱的密码，这样，就可以享用因特网上的 E-mail 服务了。只要知道对方的 E-mail 地址，就可以通过网络传输任何信息，用户可以方便地接收和转发信件，在使用 E-mail 时，会发现它有很多实用功能和技巧，例如：回信、转发信件、给多人发送信件、延迟发信、信件管理编辑以及插入附件等，这些都需要在使用过程中，不断去掌握。

使用电子邮件，每一个用户都有独自的且唯一的地址，并且格式是固定的。电子邮件地址是由一个字符串组成的，格式为 username@hostname。其中，username 是邮箱的用户名，hostname 是邮件服务器的域名。

在大多数计算机上，电子邮件系统使用用户账号或登录名作为邮箱的地址。例如某一个电子邮件地址：gary@163. com，它标识了在域名为 163. com 的计算机上，账号为 gary 的一个电子邮件用户。

注意：电子邮件地址中@是必不可缺少的组成部分，按 Shift＋2 键可得到@字符，@前面是用户名，@后面是“全称域名”，各字母之间不能有空格，前面是机器名和机构名，后面是地域类型或地域简称。

E-mail 系统中有两个服务器。发信服务器，它的功能是帮助用户把电子邮件发出去，就像发信的邮局；收信服务器，它的功能是接收他人的来信并且把它保存起来，随时供收件人阅读和变更，就像收信的邮局，模仿普通邮政业务，通过建立邮政中心，在中心服务器上给用户分配电子信箱，也就是在服务器的硬盘上，划出一块区域，相当于邮局，在这块存储区内又分成许多小区，就是邮箱。使用电子邮件的用户都可以通过各自的计算机或数据终端编辑信件，通过网络送到对方的邮箱中，对方用户可以方便地进入 E-mail 系统读取他自己邮箱中的信件。一方面，正是由于发信服务器的存在，在给对方发送邮件时，不管对方是否在线上，邮件都会先发送到邮件系统中的发信服务器，然后再由发信服务器将其发送到对方邮件系统的收信服务器中相应的邮箱内，当对方开机上线时，随时可以读取或将其下载到本地。另一方面，正是由于收信服务器的存在，对方在发送邮件时，不管是否在线上，邮件都会先存入收信服务器中的邮箱内，当用户开机上线时，可以随时读取或将其下载到本地。

2.3.2 在线收发电子邮件

所谓在线收发电子邮件是指在主页系统中进行电子邮件的收发，要求网络一直是连通的，通过主页中的电子邮件系统直接访问邮件服务器。具体步骤如下：

(1) 拨号上网后，在 IE 中访问网易主页 www. 163. com，单击邮件系统的超链接，进入邮件登录页面，在“用户名”位置输入账号，如 vivian666，在“密码”位置输入申请账号时设置的密码，然后单击“登录”按钮，如图 2-26 所示。

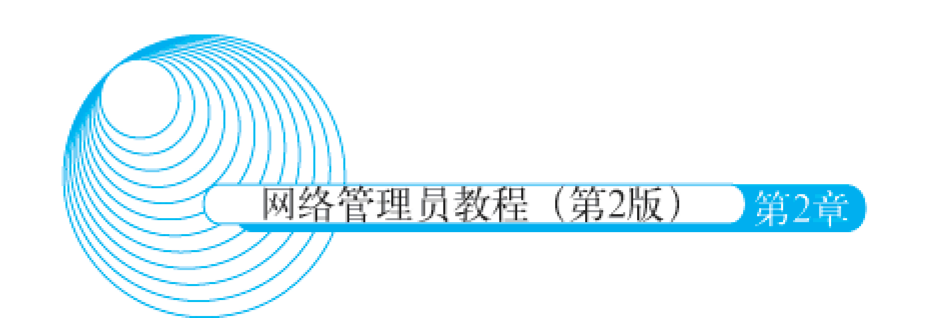


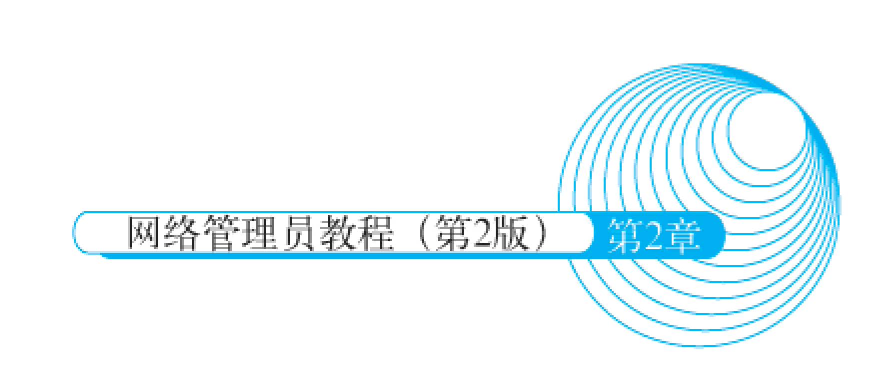


图 2-26　登录页面

（2）在邮箱页面中看到“收件箱”中有 1 封新邮件，如图 2-27 所示，单击“收件箱”链接，进入收件箱页面。



图 2-27　邮箱页面



(3) 在“收件箱页面”中看到有一封“发件人”为 Netease. com Inc 的信，如图 2-28 所示。单击这封信，进入“读邮件页面”。



图 2-28　收件箱页面

(4) 可以在读邮件页面中看到信的标题、内容、发件人地址、发送时间等信息，如图 2-29 所示。

(5) 单击邮件目录中的“发邮件”，进入“写邮件页面”，填写收件人的 E-mail 地址、主题、正文等内容，也可单击“附件”按钮将本地硬盘的文件以附件形式插入，邮件写好后，单击“发送”按钮，如图 2-30 所示。

(6) 几秒或几十秒后(具体时间取决于邮件内容和附件的大小)，会出现“邮件发送成功页面”，如图 2-31 所示。

2.3.3　利用 Outlook Express 处理电子邮件

1. Outlook Express 简介

Outlook Express 是 Microsoft 公司开发的应用最广泛的，专门用于管理电子邮件、新闻组的应用软件。Outlook Express 有以下一些优点：

(1) 可以脱机处理邮件，有效利用联机时间，降低了上网费用。可以将邮件下载到本地硬

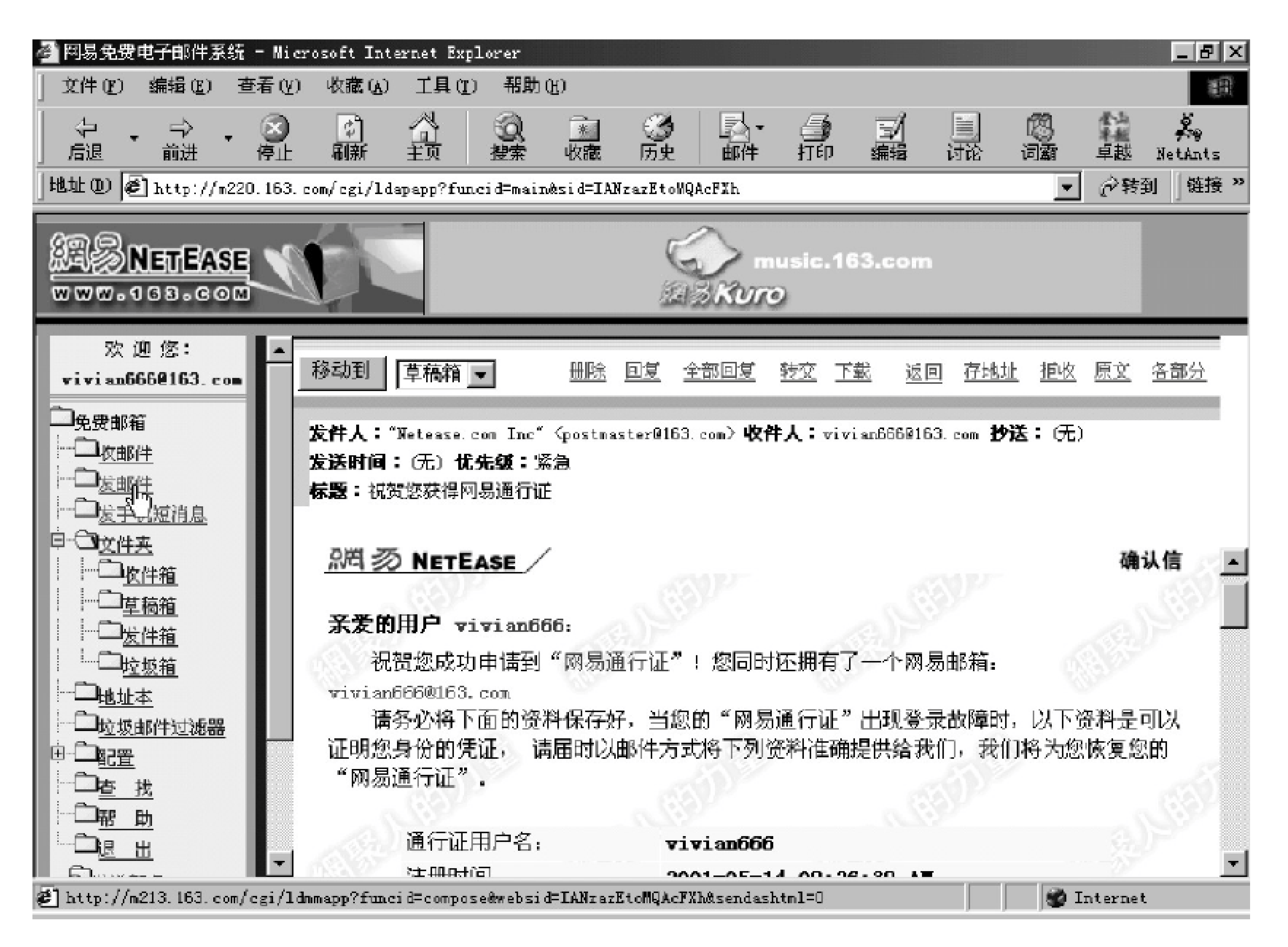


图 2-29 读邮件页面



图 2-30 写邮件页面



图 2-31 邮件发送成功页面

盘，无须连接到 ISP 就可以阅读，另外还可以脱机撰写邮件，然后在下次连接时发送出去。

（2）可以管理多个邮件账号，在同一个窗口中使用多个邮件账号。

（3）可以使用通讯簿存储和检索电子邮件地址。通过从其他程序导入、直接输入或从接收的邮件中添加等方式，就能够将邮件地址自动保存在通讯簿中。

（4）在邮件中添加个人签名或信纸。可以将重要的信息作为个人签名的一部分插入到发送的邮件中，而且可以创建多个签名以用于不同的目的。如果需要提供更为详细的信息，也可以在其中加入一张名片。为了使邮件更加美观，还可以添加信纸图案和背景，或改变文字的颜色和样式。

（5）发送和接收安全邮件。可使用数字标识对邮件进行数字签名和加密。对邮件进行数字签名可以使收件人确认邮件确实是发送的，而加密邮件则保证只有期望的收件人才能阅读该邮件。

2. 在 Outlook Express 中创建电子邮件账号

使用 Outlook Express 处理电子邮件的前提是，利用从 ISP 处得到的电子邮件账号的相关信息，在 Outlook Express 中创建电子邮件账号。具体步骤如下。

(1) 启动 Outlook Express，选择“工具”菜单下的“账号”选项，如图 2-32 所示。



图 2-32　账号菜单

(2) 选择了“账号”菜单，会弹出“Internet 账号”对话框，在该对话框中选择“添加”按钮下一级的“邮件”选项，如图 2-33 所示。

(3) 弹出“Internet 连接向导”对话框，在“显示姓名”文本框中输入名字，此名字和邮件账号没有必然联系，只是作为将来发送邮件时“发件人”的名字。例如，此处输入：Vivian，然后单击“下一步”按钮，如图 2-34 所示。

(4) 在弹出的“Internet 连接向导”对话框中，选择单选按钮“我想使用一个已有的电子邮件地址”，在“电子邮件地址”文本框中输入 vivian666@163.com，然后单击“下一步”按钮，如图 2-35 所示。

(5) 在弹出的“Internet 连接向导”对话框中，在“我的接收邮件服务器是”下拉式列表框中选择“POP3 服务器”，在“接收邮件服务器”文本框中输入接收邮件服务器的全称域名 pop.163.com，在“外发邮件服务器”文本框中输入外发邮件服务器的全称域名 smtp.163.com，然后单击“下一步”按钮，如图 2-36 所示。

说明：通常，这两个服务器的域名一般由 ISP 提供，如果是免费邮箱，则在邮箱申请成功时，由 ISP 在祝贺邮箱申请成功的页面、电子邮件或电子邮件系统登录页面中提供。

(6) 弹出“Internet 连接向导”对话框，在“账号”文本框中输入电子邮件地址@前面的部分，



图 2-33 “Internet 账号”对话框——添加“邮件”服务



图 2-34 “Internet 连接向导”对话框——输入姓名



图 2-35 “Internet 连接向导”对话框——输入电子邮件地址

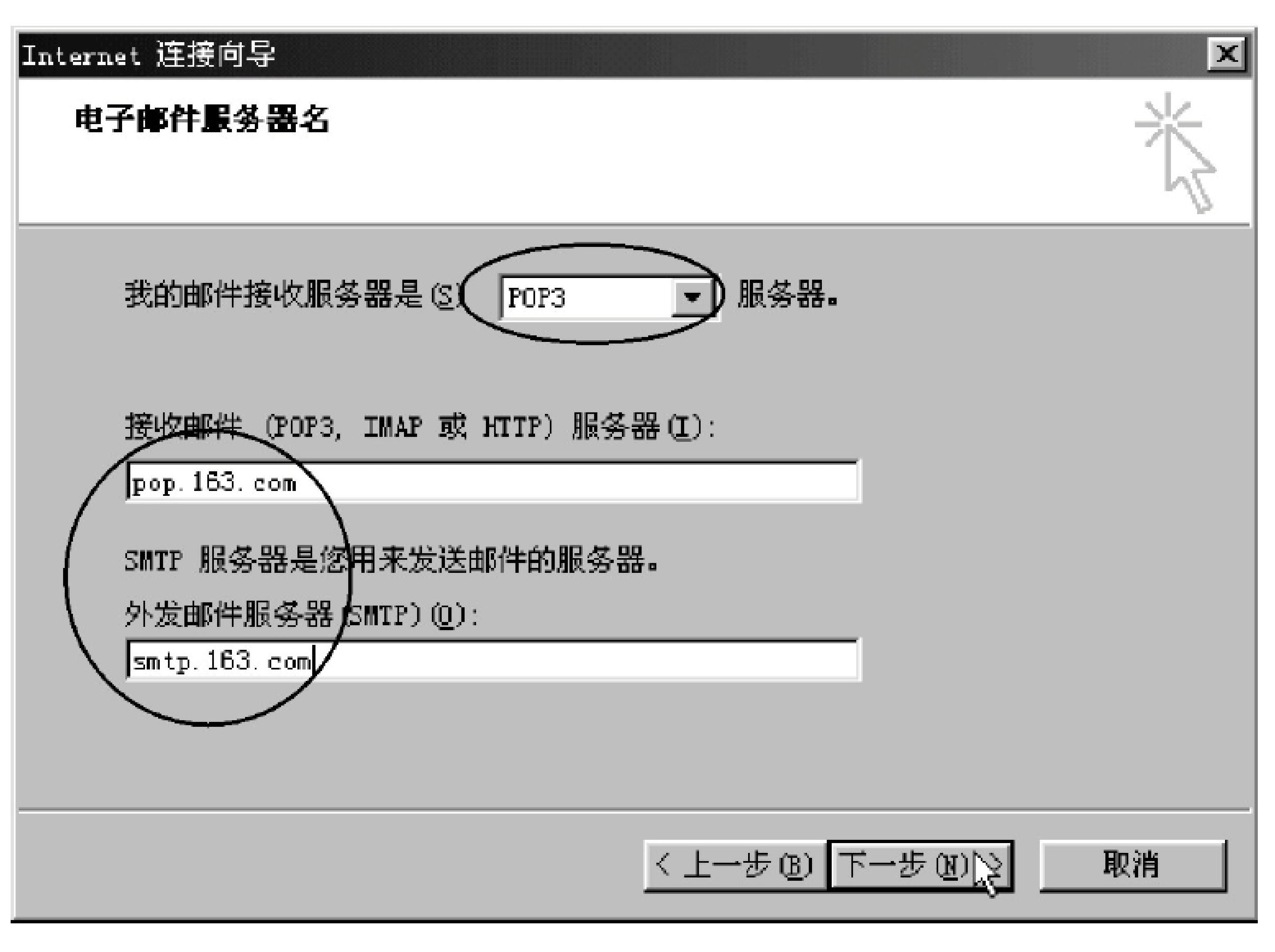


图 2-36 “Internet 连接向导”对话框——输入邮件服务器名

本例输入 Vivian666，在“密码”文本框位置输入电子邮件地址的密码，然后单击“下一步”按钮，如图 2-37 所示。

（7）在弹出的“Internet 连接向导”对话框，单击“完成”按钮。系统返回“Internet 账号”对话框，在对话框中增加了一个类型为“邮件”的账号 pop.163.com，如图 2-38 所示，单击“关闭”按钮

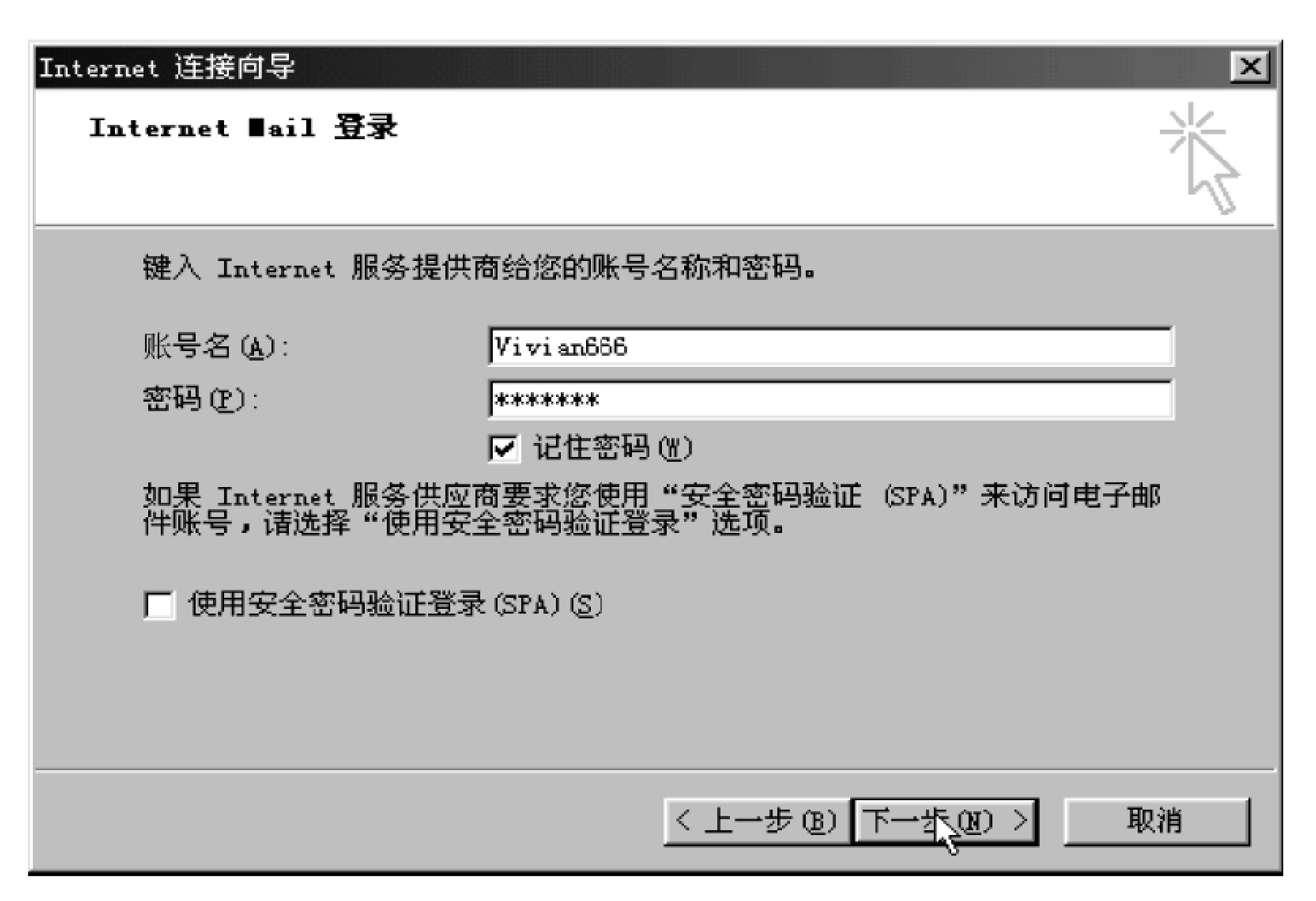


图 2-37 "Internet 连接向导"对话框——输入账号和密码



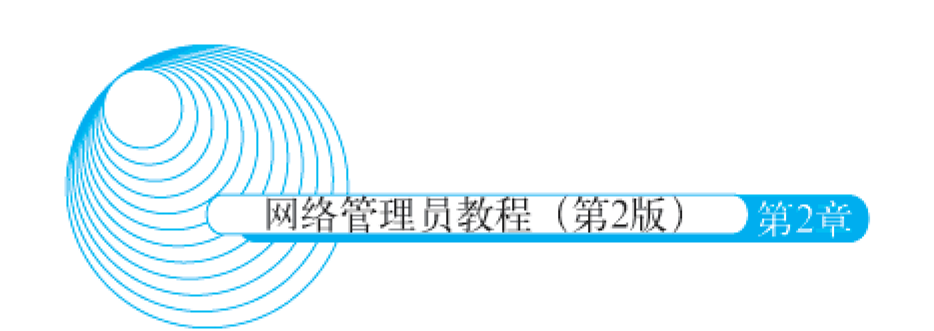
图 2-38 "Internet 账号"对话框——"邮件"服务设置完成

返回。

3. 在 Outlook Express 中收发电子邮件

(1) 单击 Outlook Express 窗口工具栏上"新邮件"按钮，如图 2-39 所示，进入写邮件窗口。

(2) 在写邮件窗口中，输入收件人的电子邮件地址、主题、正文，如果要同时发送附件，单击写邮件窗口工具栏上的"附加"按钮，插入附件，如图 2-40 所示。



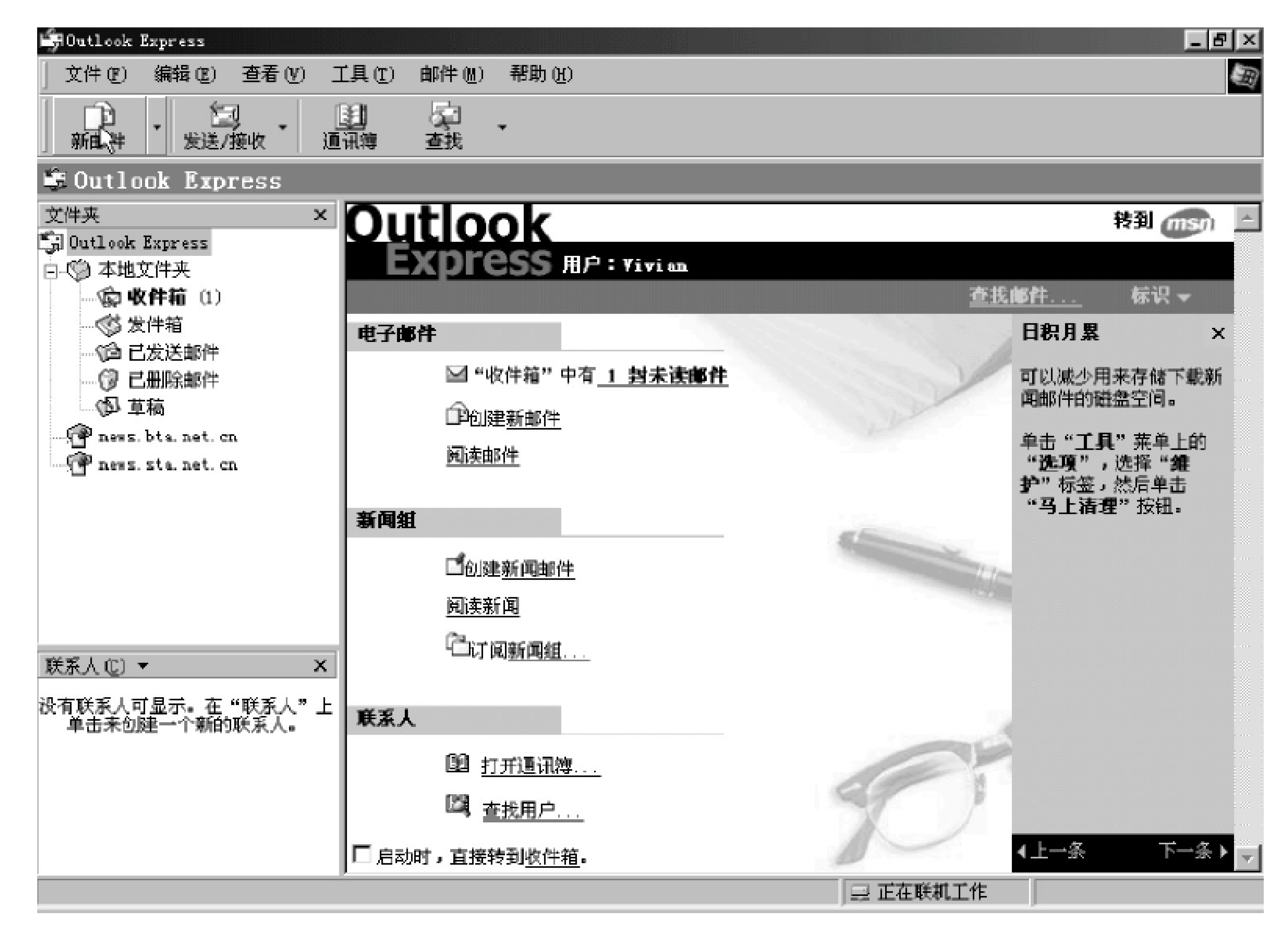


图 2-39　Outlook Express 窗口——单击“新邮件”工具按钮

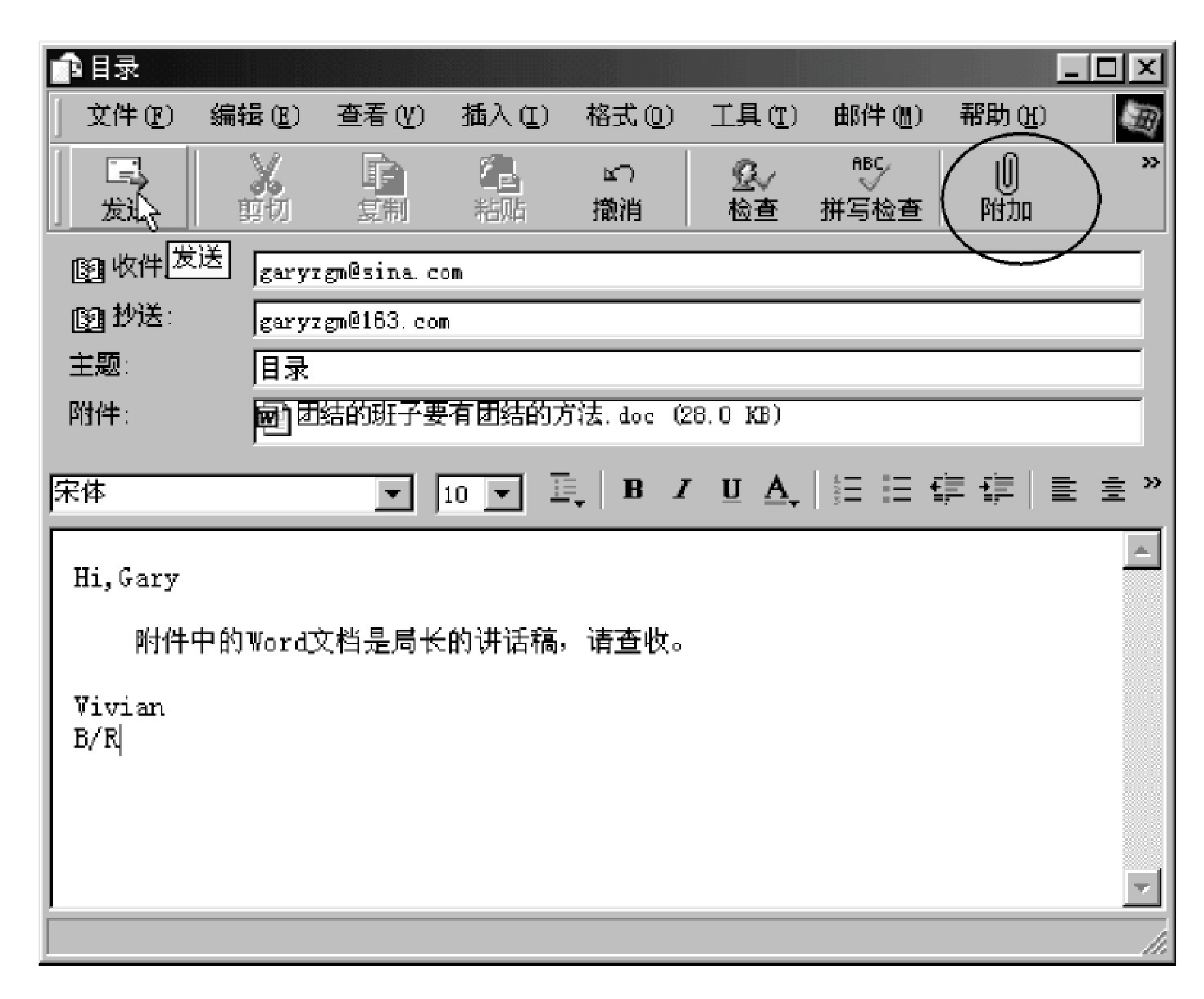


图 2-40　写邮件窗口

（3）在“插入附件”对话框中，通过浏览选择拟插入附件后，单击“附件(A)”按钮，将附件加入到邮件中，如图 2-41 所示。

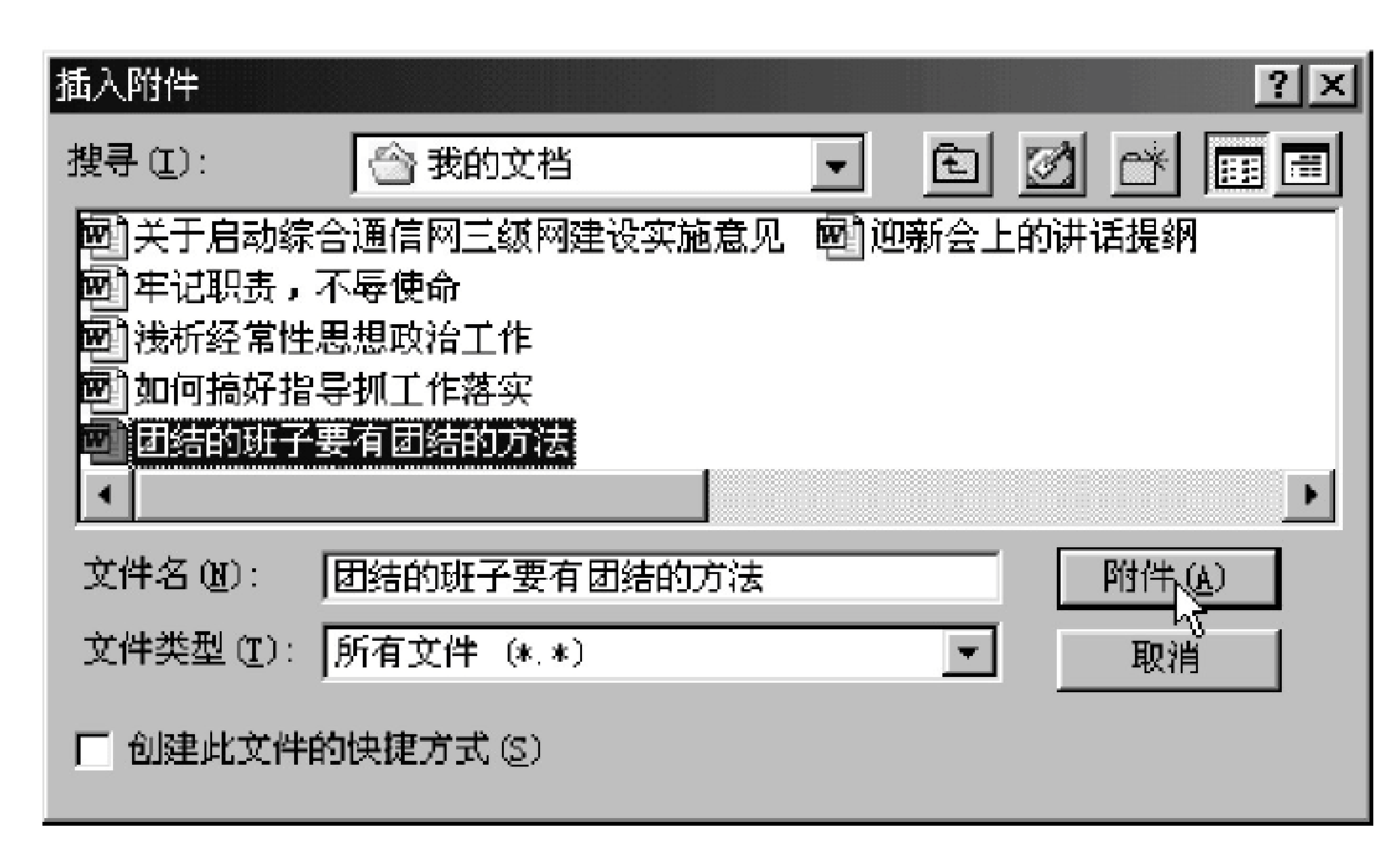


图 2-41 “插入附件”对话框

（4）当邮件书写编辑完毕后，单击写邮件窗口工具栏上的“发送”按钮(见图 2-40)，将邮件发送到“发件箱”(本地硬盘的一个文件夹)。执行了发送命令后，“发件箱”中多了一封待发送邮件，如图 2-42 所示。需要说明的是，在此之前都不要求在线。

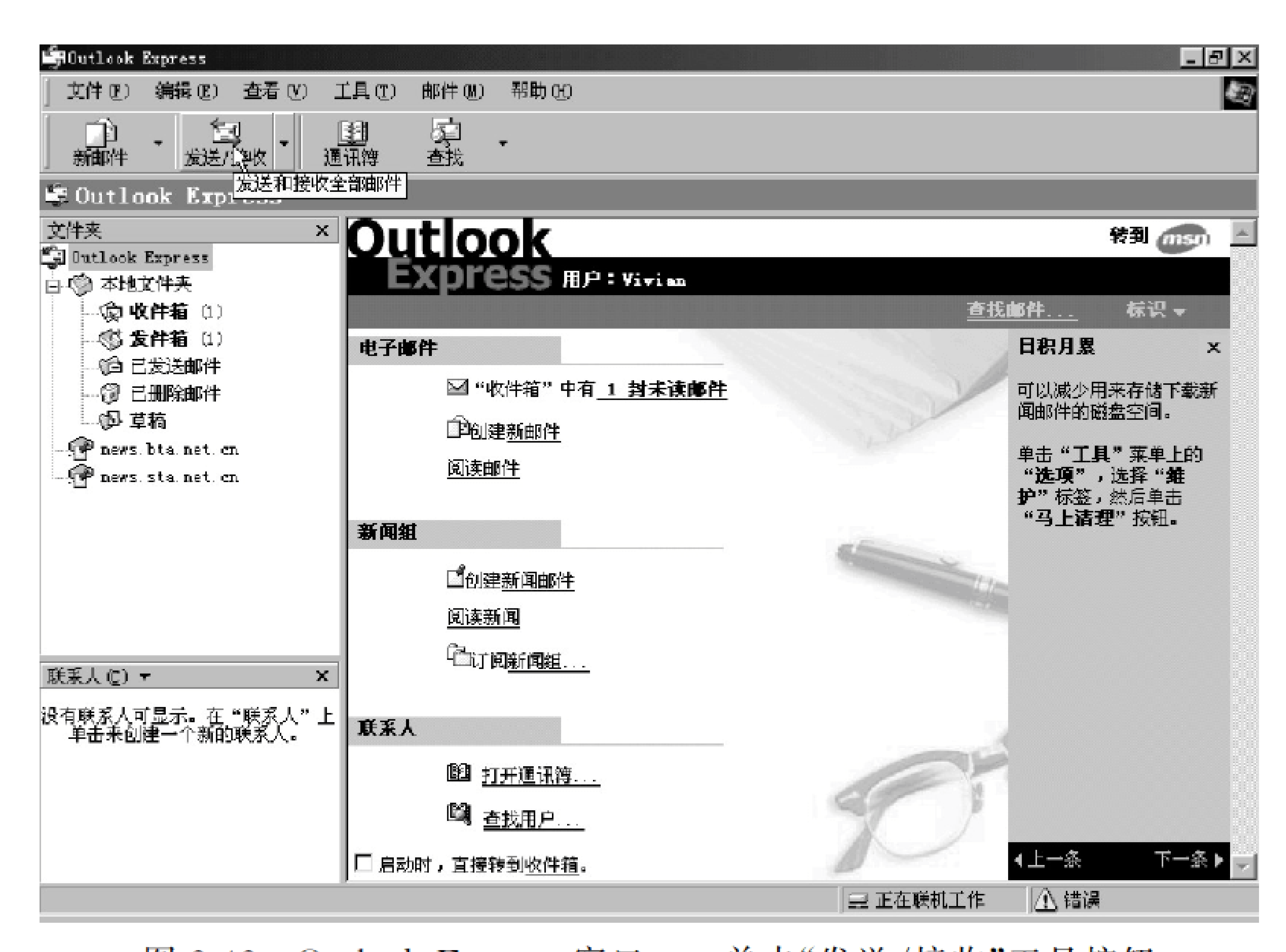


图 2-42 Outlook Express 窗口——单击“发送/接收”工具按钮

（5）拨号上网，网络连通后，单击 Outlook Express 窗口工具栏上“发送/接收”按钮（见图 2-42），这时，出现邮件“传输提示”对话框，如图 2-43 所示。传输完成后，“传输提示”对话框关闭（具体传输时间取决于发送和接收的邮件内容和附件的大小）。

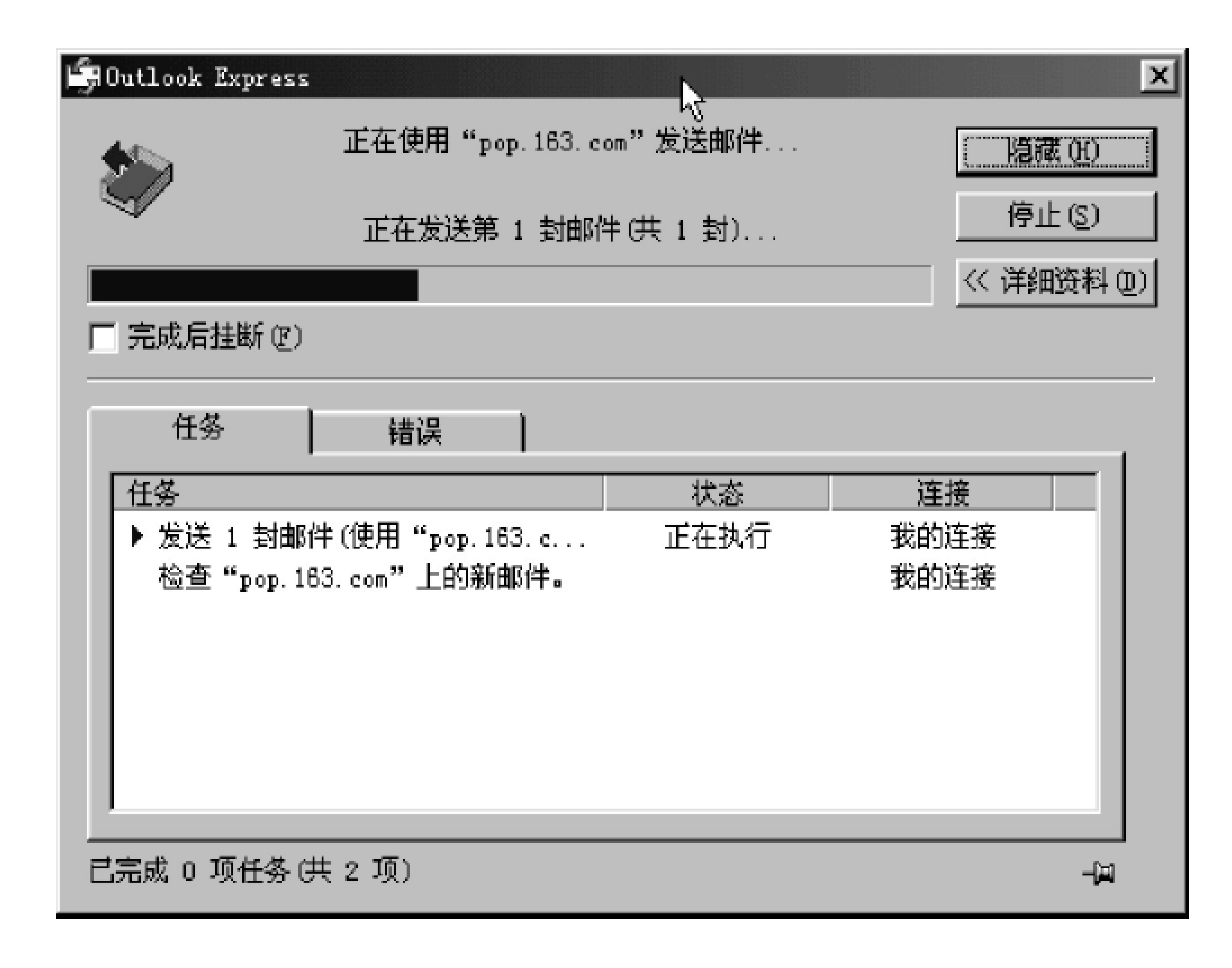


图 2-43　电子邮件传输提示对话框

（6）此时，可以断开网络连接，看到“发件箱”中的那封待发送邮件没有了，“收件箱”中的信件由 1 封变为 2 封，多了一封刚刚接收的邮件，如图 2-44 所示。

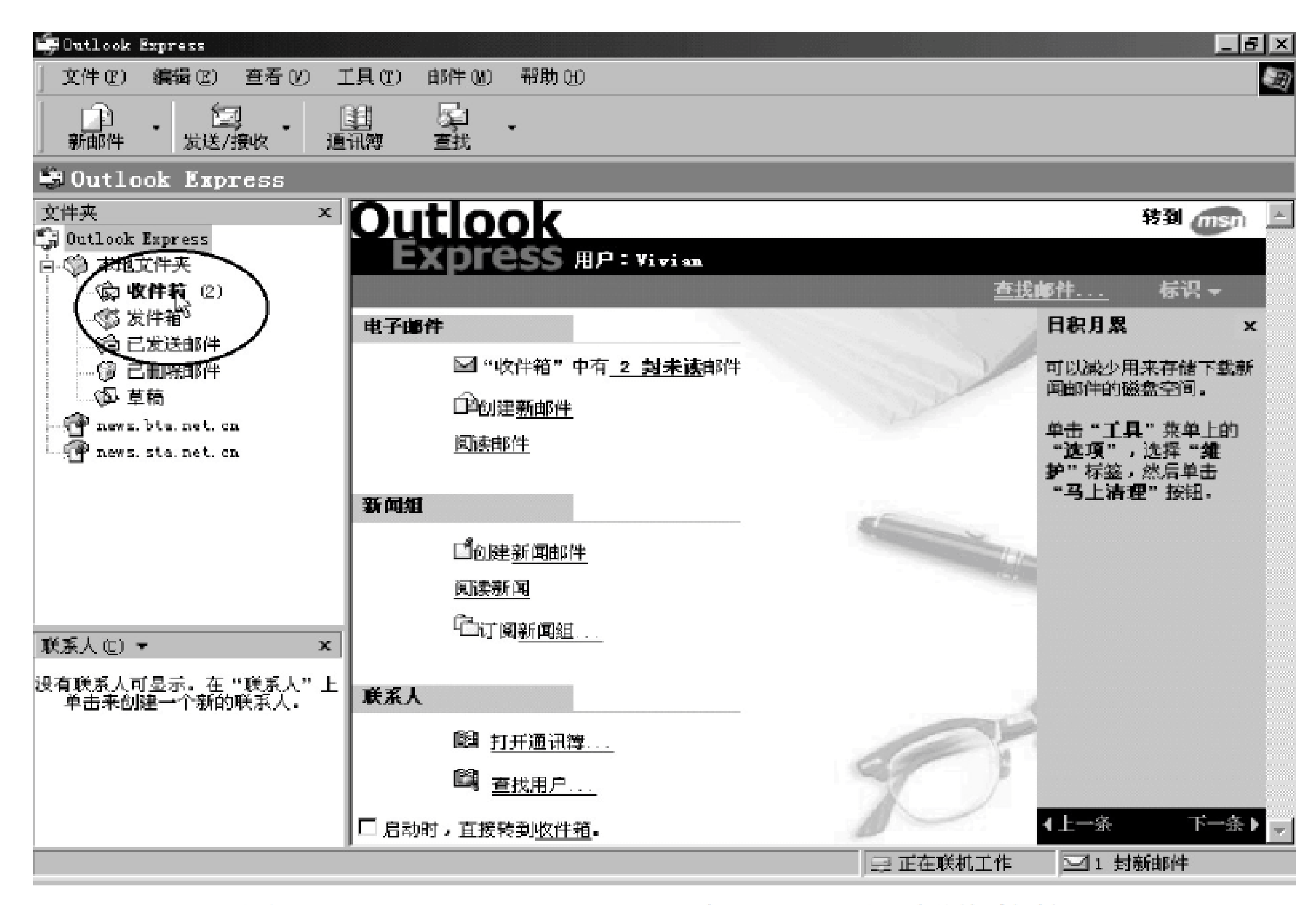


图 2-44　Outlook Express 窗口——查看“收件箱”

（7）单击“收件箱中有 2 封未读邮件”，进入读邮件窗口，选择“发件人”为 garyzgm 的邮件，可进一步查看该邮件内容，这封邮件的信息栏中带有回形针符号 ，表示该邮件中插有附件，如图 2-45 所示。



图 2-45 读邮件窗口

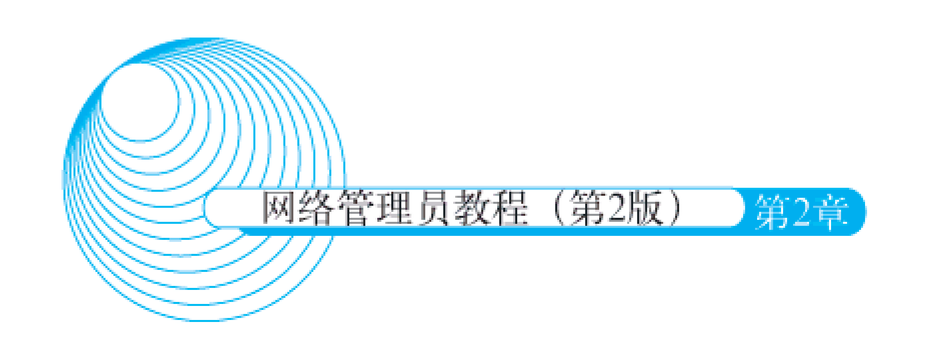
在读电子邮件时，有时收到的信中有古怪字符，这是电子邮件的乱码现象。这是因为在因特网上使用的中文编码未统一，中国内地通常使用的编码方式是 CN-GB 简体中文标准，在港、澳、台以及东南亚通常使用 BIG-5 码繁体中文。遇到乱码不必紧张，可以改用另外一种汉字标准，在 IE、Outlook 或 Outlook Express 中，使用“查看”菜单“编码”选项中的“其他”，在列表中选择一个编码标准，一般来讲，就可以消除 E-mail 中的乱码了。

2.4 文件传输协议

2.4.1 FTP 基本概念

1. 什么是 FTP

FTP(File Transfer Protocol)中文译为文件传输协议，是因特网上的另一项主要服务，这项服务的名字是由该服务使用的协议引申而来的，各类文件存放于 FTP 服务器，可以通过 FTP 客



户程序连接FTP服务器，然后利用FTP协议进行文件的“下载”或“上传”。

所谓下载就是通过相应客户程序，在文件传输协议的控制下，将因特网共享文件服务器中的文件传回到本地计算机中，这个传回文件的过程就称为下载(Download)。除此之外，也可以将本地计算机中的文件传送到FTP服务器上，这个过程便称为上传(Upload)。

2. 匿名FTP(Anonymous FTP)

连接FTP服务器，大都要经过登录(Login)的过程，也就是输入在该服务器上申请的账号和密码，其目的是要让FTP服务器知道是谁登录进来使用该主机。由于FTP服务相当热门，为了方便使用者，大部分FTP服务器都提供了一种称作Anonymous FTP(匿名FTP)的服务，使用者不需要申请主机的特殊账号及密码，即可进入FTP主机，任意浏览及下载公共文件。在使用匿名FTP时，只要以anonymous作为登录的账号，再用电子邮件地址作为密码即可进入主机。使用匿名FTP进入某主机时，通常只能下载文件，而无法上传文件到该主机或修改主机中的文件。不过有些主机的管理者，为了让大家有机会发表自己的文件或软件，会在FTP主机上建立一些目录，即使是以匿名的方式登录，也可以自由地上传或修改这些目录下的文件。

3. FTP客户程序

访问FTP服务器的客户机上必须装有专门的客户程序，常见的FTP客户程序有：命令行程序FTP、图形化客户程序WS_FTP、CuteFTP或浏览器。命令行客户程序是Windows目录下的一个可执行文件FTP.EXE，执行FTP命令后，进入FTP命令环境，建立连接、下载和上传文件都需要专门的FTP命令来完成。图形化客户程序WS_FTP、CuteFTP可从网上下载安装，建立连接、下载和上传文件是在Windows的图形化界面中完成的，相对简单一些，但使用者需要安装WS_FTP程序，并学习WS_FTP的操作使用方法，和命令行客户程序一样，这两个程序在使用时都需要建立连接，输入账号进行登录，即使是匿名登录也需要输入anonymous账号进行身份验证。对比来讲，用浏览器作为FTP客户程序访问FTP服务器是最为方便的一种方法，常见的浏览器Microsoft Internet Explorer和Netscape Communicator等都可作为FTP客户程序使用，并且匿名登录时不需要输入anonymous账号进行身份验证。

注意：在浏览器URL地址栏中如果不输入服务器类型，则默认的服务器类型是http，即采用超文本传输协议的WWW服务器。在访问FTP服务器时，要指明所访问的服务的类型“ftp”。另外，在访问FTP服务器之前，通常需要知道所需要的软件或资料存放的位置。

2.4.2 FTP客户程序浏览器

下面，以IE浏览器作为FTP客户程序，访问清华大学的FTP服务器。下载“图形界面的FTP客户程序WS_FTP”。

（1）启动 IE 浏览器，在 URL 地址栏输入：ftp://ftp.tsinghua.edu.cn，连接成功后，在浏览器窗口中显示的是 FTP 服务器的目录结构，而不是 Web 页，如图 2-46 所示。

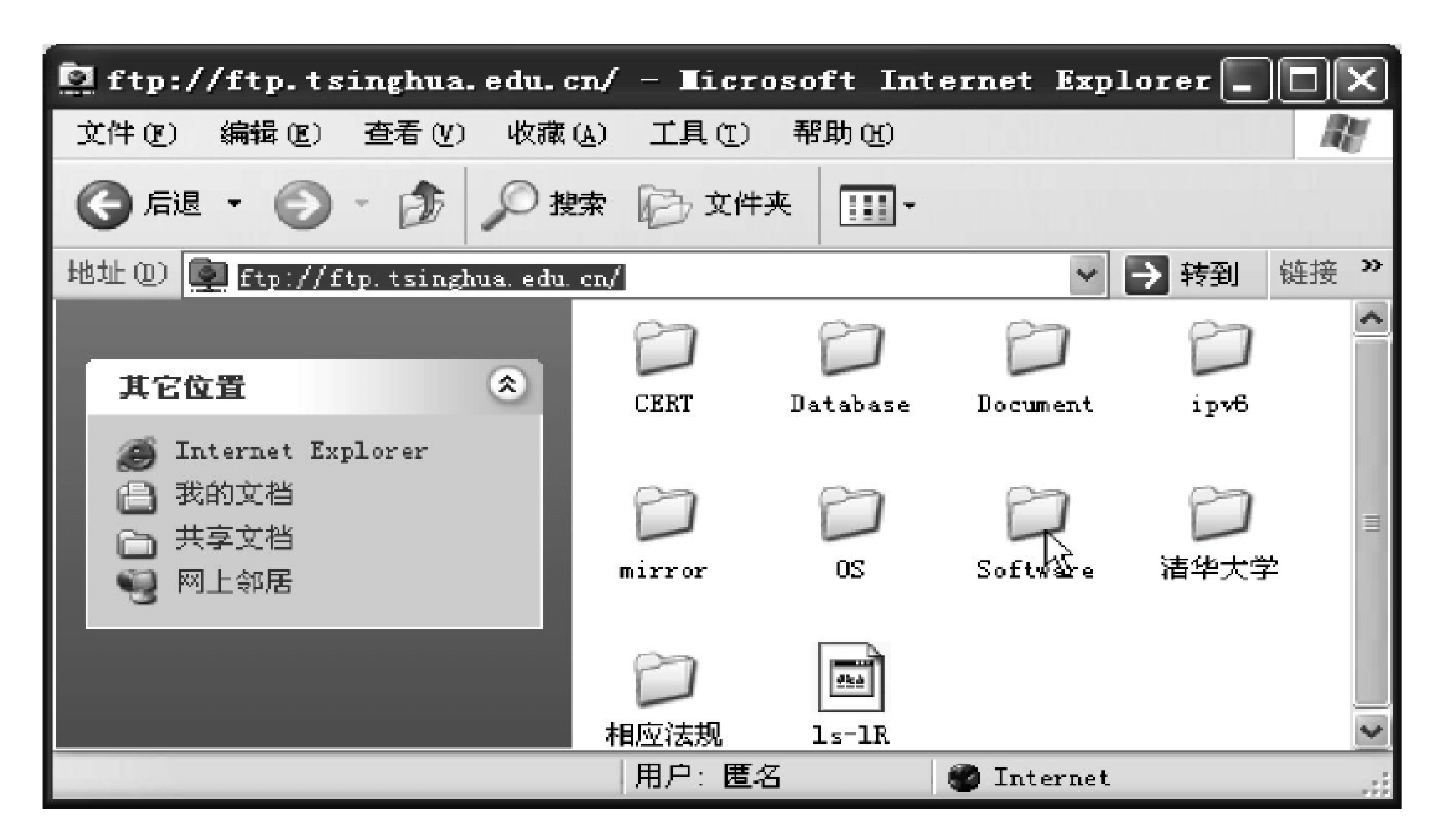


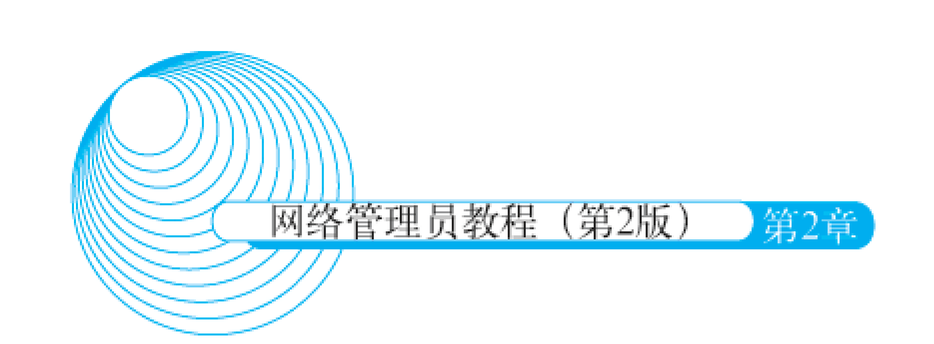
图 2-46 IE 访问 FTP 服务器窗口

（2）双击 Software 文件夹，依次进入 Network、FTP、Client、WsFTP 文件夹，如图 2-47 所示。



图 2-47 IE 访问 FTP 服务器的目录窗口

（3）找到要下载的文件 Ws_FTP.zip，双击该文件，弹出“文件下载”对话框，如图 2-48 所示。单击“保存”按钮，出现“另存为”对话框，指定下载文件存放的目录和文件名，确定后开始下载。



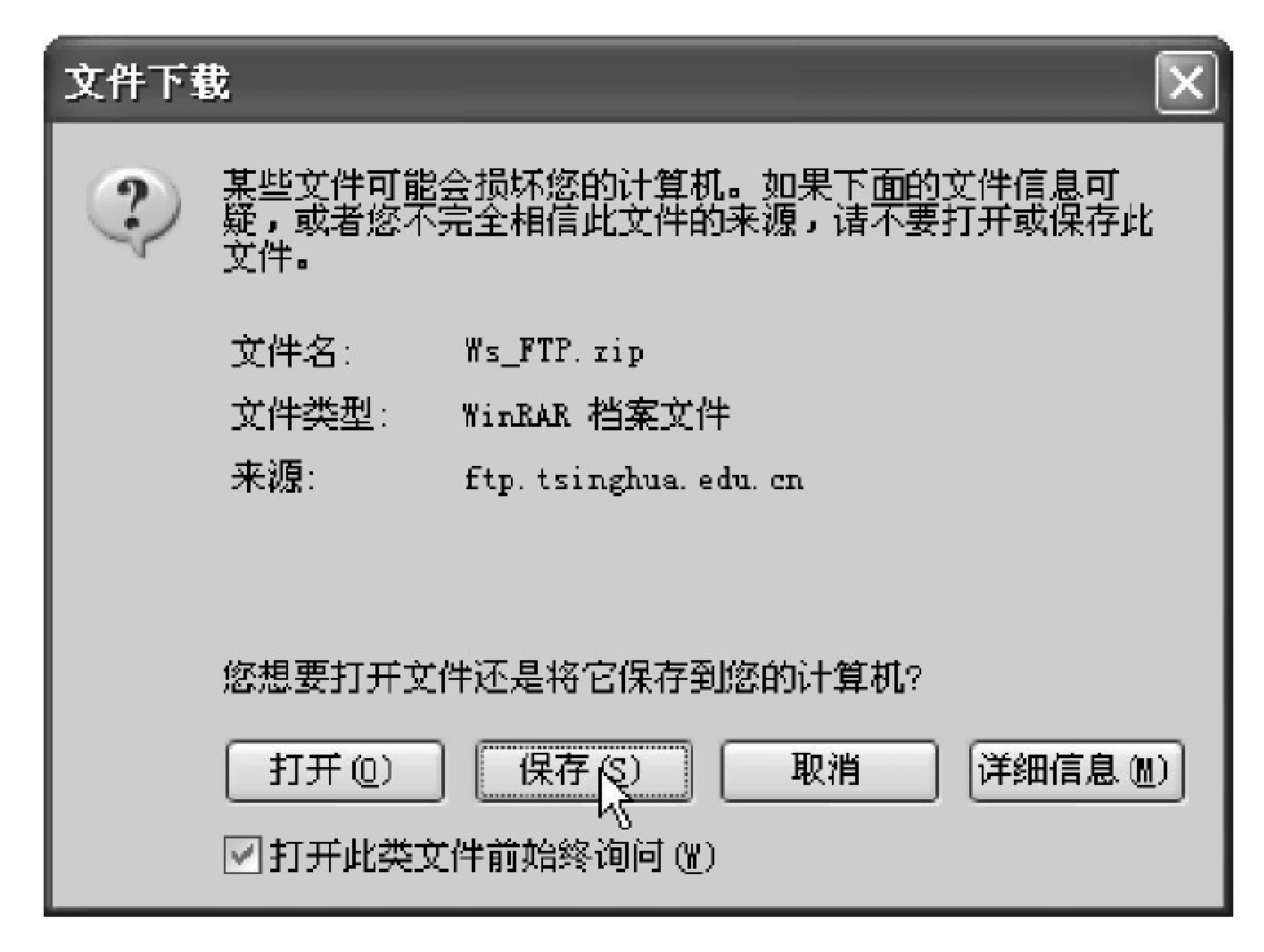


图 2-48　IE 访问 FTP 服务器的文件下载对话框

2.4.3　FTP 客户程序 FTP.exe

从使用者的角度来看，FTP.exe 是网络上互传文件的工具。只有计算机安装了 TCP/IP 协议，才能在 Windows 环境下使用这个工具。若计算机已通过拨号或专线方式连上因特网，就能方便地使用这个工具在因特网上进行文件传输来获得各种各样的共享软件。

一般情况下，应在 Windows 的命令行提示符下使用这个工具，也可以在“运行”对话框中输入 FTP，如图 2-49 所示，随即进入 FTP 命令行状态，如图 2-50 所示。



图 2-49　运行 FTP 命令

这时就可以使用 FTP 命令行工具了，通常先用 open 命令打开一个连接，把本地计算机与一个远程主机连接起来，然后用 dir 命令查看远程主机内容，用 cd 命令进入相应的目录。用 get 或 mget 下载远程主机的文件到本地计算机上。若对远程主机拥有写权限，就可用 put 或 mput 把

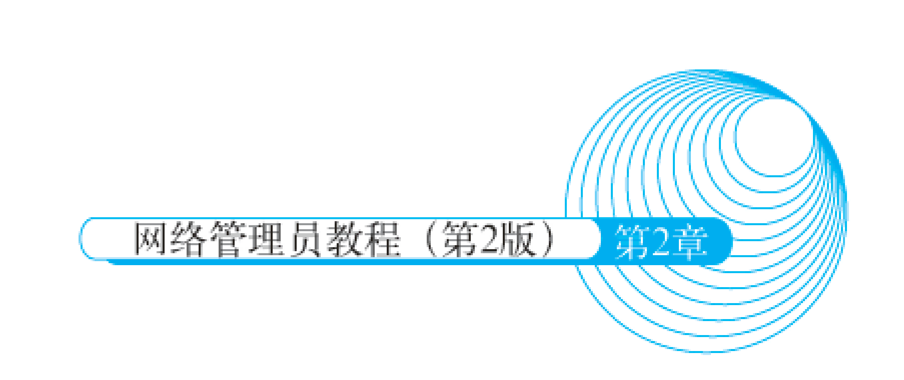




图 2-50　FTP 命令行状态

本地计算机的文件传到远程主机上。完成任务后用 close 关闭此连接，然后可用 open 打开另外一个连接或用 quit 退出 FTP。下面简要介绍一下几个重要的 FTP 命令。

1. 打开、关闭连接

1）open *Hostname* [*Port*]

这条命令的功能是把本地计算机连接到远程主机上。只有连接成功后，才能进行文件的上传和下载等工作。其中，参数 *Hostname* 是指定要连接的远程计算机，可用域名也可用 IP 地址。参数 *Port* 指定用于联系 FTP 服务器的 TCP 端口号。默认情况下，使用 TCP 端口号 21。

连接成功后，计算机会提示输入用户名（username）与密码（password）。也可输入匿名用户 anonymous 或 ftp，密码用 E-mail 地址或“FTP”代替，但匿名用户只能进行文件的下载不能进行文件的上传。

2）close/disconnect

这两条命令的功能相似，都是结束与远程服务器进行的 FTP 会话，并停留在 ftp>提示符下。

3）bye/quit

这两条命令的功能相似，都是结束与远程的 FTP 服务器会话并退出 ftp>提示符。

2. 查看信息、切换路径

1）pwd

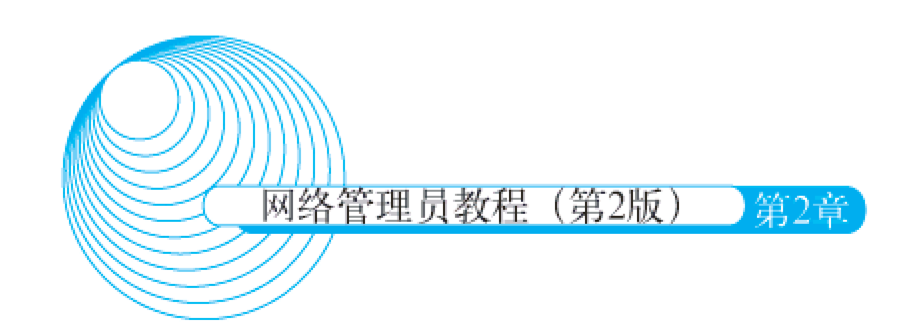
显示远程计算机上的当前目录。

2）cd *RemoteDirectory*

这条命令的功能是更改远程计算机上的工作目录。*RemoteDirectory* 是指定要更改的远程计算机上的目录。

3）lcd [*Directory*]

这条命令的功能是更改本地计算机上的工作目录。默认情况下，工作目录是启动 ftp 的目录。其中参数 *Directory* 是指定要更改的本地计算机上的目录。如果没有指定 *Directory*，将显



示本地计算机中当前的工作目录。

4）ls/dir [*RemoteDirectory*] [*LocalFile*]

这两条命令的功能相似，都是显示远程计算机上的目录文件和子目录列表。其中参数 *RemoteDirectory* 是指定要查看其列表的目录。如果没有指定目录，将使用远程计算机中的当前工作目录。参数 *LocalFile* 是指定要存储列表的本地文件。如果没有指定本地文件，则屏幕上将显示结果。

5）mkdir *Directory*

这条命令的功能是创建远程计算机上的目录。其中参数 *Directory* 是指定的新的远程目录的名称。

6）rename *FileName NewFileName*

这条命令的功能是重命名远程文件。参数 *FileName* 是指定要重命名的文件。参数 *NewFileName* 是指定的新文件名。

7）delete/mdelete *RemoteFile*

delete 命令的功能是删除远程计算机上的一个文件。mdelete 命令的功能是删除远程主机上的多个文件，支持通配符。参数 *RemoteFile* 是指定要删除的远程主机上的文件。

3．对远程主机上的文件进行操作

1）put/send/mput *LocalFile*

put 或 send 的功能是把本地计算机的一个文件上传到远程主机上。mput 的功能是把本地计算机的多个文件上传到远程主机上，支持通配符。参数 *LocalFile* 是指定要复制的本地文件。

2）get/recv/mget *RemoteFile*

get 或 recv 的功能是下载远程主机的一个文件到本地计算机上。mget 的功能是下载远程主机的多个文件到本地计算机上，支持通配符。参数 *RemoteFile* 是指定要复制到本地计算机的远程文件。

4．其他命令

1）!

该命令的功能是从 ftp 命令行提示符临时退出到 Windows 命令行提示符下，以便可以运行 Windows 命令。要返回到 ftp 子系统，在 Windows 命令行提示符下输入 exit。

2）? /help [*Command*]

这两条命令的功能相似，都是显示 ftp 命令说明。参数 *Command* 是指定需要说明的命令的名称。如果未指定 *Command*，则显示所有的命令列表。

2.4.4 FTP 客户程序 CuteFTP

前面学习了一些 ftp 基本指令，但是对于大部分用户来说，使用指令还是不太方便。现在介绍图形用户接口的 FTP 客户端软件 CuteFTP。CuteFTP 不但包括了 ftp 命令的全部功能，还包括有目录比较、宏、目录上传和下载、远程文件编辑、IE 风格的工具条、多线程文件传输、多站点同时连接、SSL 安全连接支持等。CuteFTP 软件通常可以在较大的 FTP 服务器上的/Pubpsoftware/ftp 目录下找到。

CuteFTP 的运行窗口如图 2-51 所示，在“主机”栏中输入待连接的远程主机的 IP 地址或域名，在“用户名”栏和“密码”栏中分别输入远程主机合法的 FTP 用户名及其密码，然后按 Enter 键即可与远程主机相连。

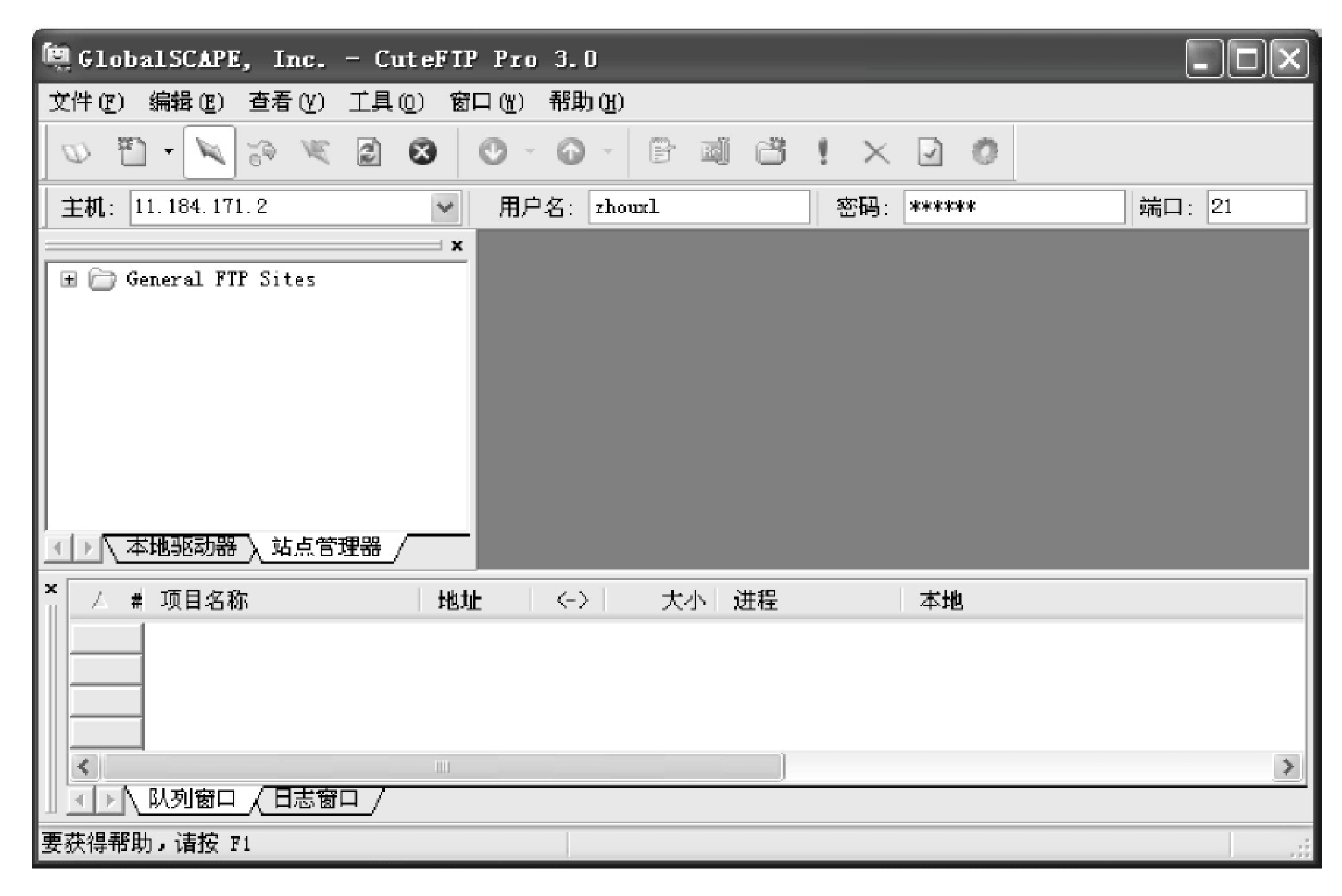


图 2-51　CuteFTP 初始界面

与远程主机连接后，远程主机的相关信息会在 CuteFTP 窗口中显示，如图 2-52 所示。通常窗口左边区域显示的是本地硬盘中的文件信息，也可以认为是本地主机窗口。窗口右边区域显示的是远程主机的 FTP 用户的家目录，也可以认为是远程主机窗口。另外，在下面还有用于对下载、上传项目进行管理的队列窗口和记录下载、上传信息的日志窗口。

使用 CuteFTP 进行文件的下载和上传十分方便，下载文件时，只须在远程主机窗口中双击待下载的文件即可，或者用鼠标的右键单击待下载的文件或文件夹，在弹出的快捷菜单中选择“下载”命令，如图 2-53 所示。

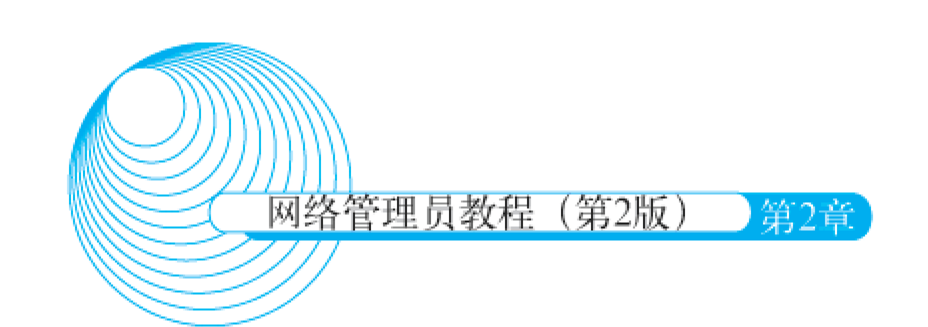


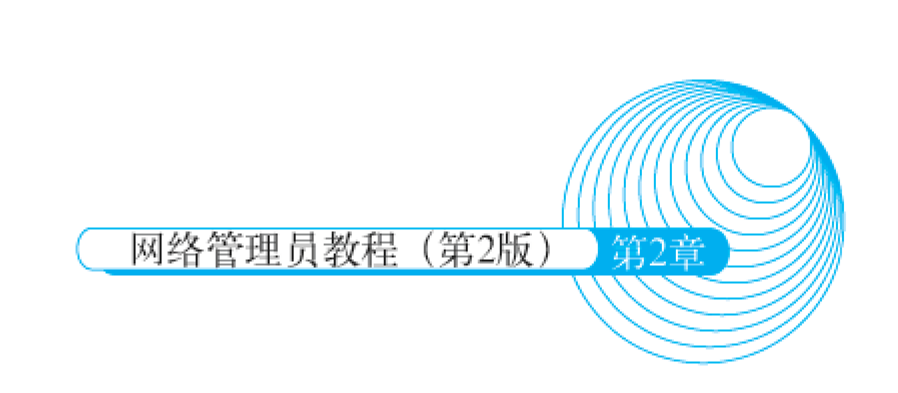


图 2-52　远程连接后的 CuteFTP 窗口



图 2-53　文件下载

上传文件时，只须在本地主机窗口中双击待上传的文件即可，或者用鼠标的右键单击待上



传的文件或文件夹，在弹出的快捷菜单中选择“上传”命令，如图 2-54 所示。

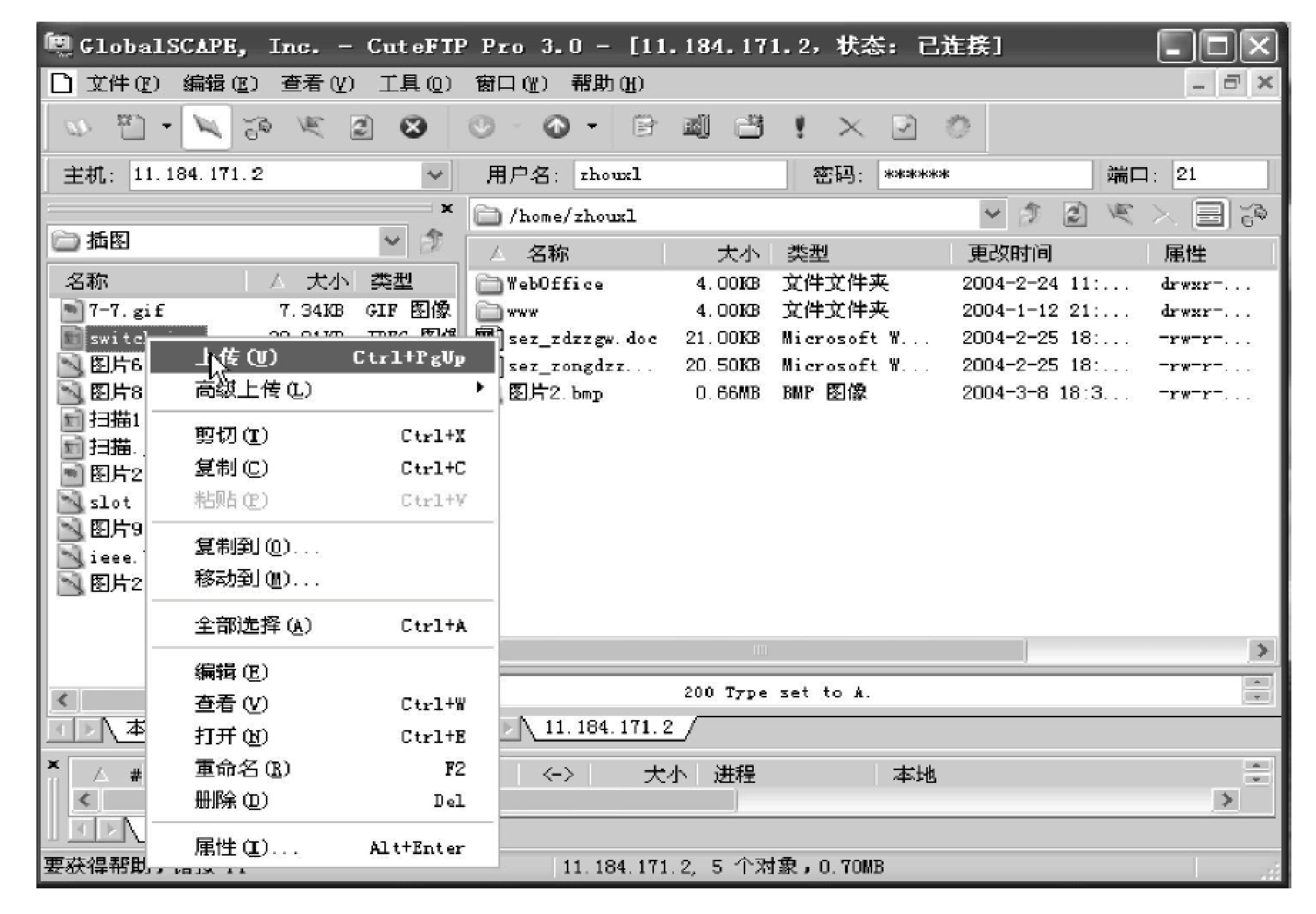


图 2-54 文件上传

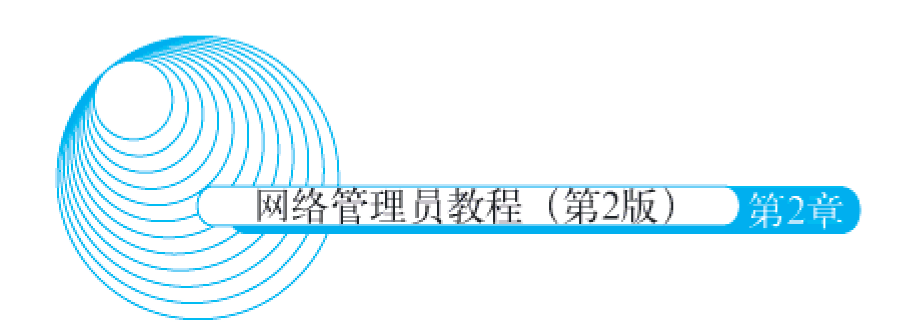
当然，CuteFTP 也支持 Windows 的剪贴板操作，在本地主机窗口和远程主机窗口都可以执行“复制”、“剪切”、“粘贴”命令。

2.5 其他因特网应用

2.5.1 BBS

BBS 是 Bulletin Board System 的缩写，翻译过来就是电子公告板。BBS 是 Internet 上著名的，也是最常用的信息服务系统之一。BBS 发展非常迅速，几乎遍及整个 Internet。提供 BBS 服务的系统叫做 BBS 站，它们各具不同的风格和特色。BBS 站为用户开辟一块展示“公告”信息的公用存储空间作为“公告板”，就像实际生活中的公告板一样，用户们在这里可以围绕某一主题开展持续不断的讨论，人人都可以把自己参加讨论的文字“张贴”在公告板上，也可以从中读取其他参与者“张贴”的信息。BBS 具有一些共同的基本功能，如：信件交流、文件传输、信息交流、经验交流及资料查询等。

访问 BBS 站点使用的软件可以是远程登录程序 Telnet，也可以是专用的 BBS 终端软件 NetTerm 或 CTerm。例如，使用 Telnet 访问清华大学的水木清华 BBS 站点，具体步骤如下。



（1）首先连通网络，然后用 telnet 软件登录 BBS 主机。选择 Windows 的“开始”按钮下的“运行”，然后在打开命令栏中输入 Telnet bbs. tsinghua. edu. cn

（2）随后进入在 BBS 系统主画面，如图 2-55 所示。在此需要输入 BBS 系统的用户代号，这个代号将是在各 BBS 栏目里的标识。代号 guest 是以“过客”的身份登录进入 BBS 系统，其权限受到一定限制。如果要享有足够的权限，可输入 new 去申请一个新的 BBS 系统代号，不过一般需要 3 天的系统认证时间。在此以代号 guest 的身份登录，进入 BBS 系统。



图 2-55　水木清华 BBS 系统主画面

（3）登录进入 BBS 系统后，可按系统提示进入感兴趣的相关内容。

需要指出的是，随着 HTML 技术的发展，BBS 站点目前也提供 Web 方式的用户界面，如图 2-56 所示。访问 Web 方式的 BBS 站点就不用远程登录软件 Telnet 的命令行界面了，而是使用图形用户界面的浏览器，互动操作更为简单快捷。

2.5.2　网络新闻组

网络新闻组（UseNet）就是 User’s Network，即用户交流网，它是一群有共同爱好的 Internet 用户为了相互传递交换信息组成的一种无形的用户交流网。可以把 UseNet 看成是一个有组织的电子邮件系统，不过在这里传送的电子邮件不再是发给某一个特定的用户，而是全世界范围内的新闻组服务器。UseNet 不是一个网络，而是 Internet 上的一种服务，它作为全世界最大的电子布告系统，其服务器遍布世界各地，向各种用户提供他们想要的任何新闻。在这个布告栏上任何人都可以贴布告，也可以下载其中的布告，UseNet 用户写的新闻被发送到新闻组后，任何访问该新闻组的人都有可能看到这个新闻。

UseNet 是讨论性质的，它允许世界上任何地方的用户参与。由于新闻组的用户常常利用新闻组的公平开放和 Internet 的快速高效的特点，在新闻组上提出自己在生活、工作中的问题，

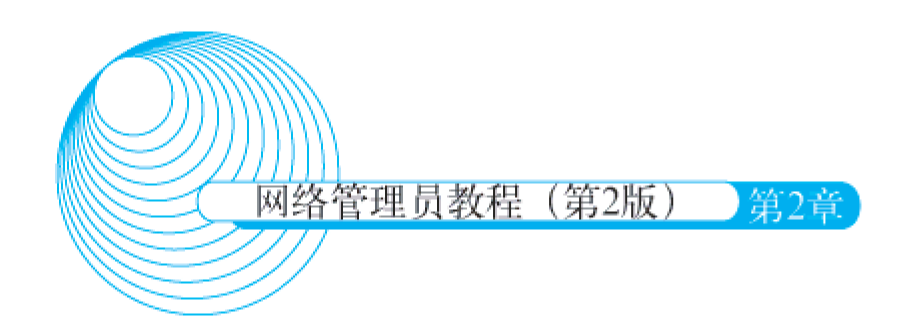


图 2-56　水木清华 BBS 系统 Web 站点

发布自己有关学术、商业以及其他一切感兴趣的观点，这使得新闻组就像一个世界性的聊天广场，其话题覆盖了令人难以置信的各种主题，在这里会发现你所能想象到的任何聊天话题。几乎任何一个古里古怪的问题，都可以在 UseNet 上问问，也许很快就能得到一个非常满意的答复。其实网络新闻并无一个确定的消息提供者，而是由使用网络新闻的每一个用户提供。比如，上网看新闻，发现了一篇感兴趣的文章，想谈谈自己的想法，于是就写了一篇表白自己看法的文章，然后贴到刚才看到的文章中。该文章经过网络新闻服务器，几分钟或几小时就可让世界各地的人们在网络上看到。当然在世界某一角落，有人对该文章有意见，于是也发表了一些看法，同样贴出来。当然，也可以提供新的信息，贴出来与大家分享、讨论。就是这样一种运作方式，使得网络新闻生生不息，每个时刻都有新的信息从世界各地发出。

网络新闻是分门别类的，用户依照自己的需要，可以选择适合自己的新闻组(Newsgroup)，收看新闻或发表意见。网络新闻是按照不同的专题分类组织的，每一类为一个专题组，通常称为新闻组，其内部又分为若干子专题，子专题下还可以有子专题。目前已经有了成千上万个新闻组，热门的 UseNet 新闻组有以下几大类：

- comp　计算机科学及相关的话题
- news　一般性的新闻话题



- rec 个人爱好、娱乐活动、艺术话题
- sci 科学研究、工程技术
- soc 社会类话题
- biz 商业类话题
- talk 有争议的话题
- misc 不属于以上几类的或有交叉的话题

后来又增加了一类“alt”，这是一个范围较小、使用的人也较少的一个新闻组，“alt”是“alternative”的简写，是“替代”的意思，在这个组可以讨论各类话题。

这些分类只是将新闻内容按其涉及的领域粗略地加以区分，远不能满足人们方便查找的要求，为了帮助区分不同的新闻组，还要将新闻组名分为几个等级。第一级就是上面的类型名，以下各级给出话题的范围，用以标识新闻的更小范围，各分类名之间用“.”隔开，使人一看到该新闻组名称，就可以确定其主题的含义，例如：

- rec. audio 是讨论声音系统的新闻组。
- sci. biology 是讨论生物学的新闻组。
- comp. os. windows 是讨论 Windows 操作系统的新闻组。
- comp. os. windows. apps. wordproc 是讨论 Windows 操作系统下字处理软件的新闻组。

从规则上讲，新闻组名的分类可以非常具体，因为其分层没有限制，但是在实际应用中，不常用的新闻组可能只有一个标题，而有些新闻组名可能用到五层或更多层的新闻组名。有的时候也可能会在不同的分类中出现相同的组，只是名字的第一部分有所不同。例如：

- rec. autos. antique 是娱乐类有关汽车爱好者的讨论。
- sci. autos. antique 是科技类有关汽车爱好者的讨论。

这两个新闻组讨论相同的内容，只是前一个被分在娱乐类中，后一个被分在科技类中。

UseNet 的基本通信手段是电子邮件，但它不同于电子邮件的一对一通信，而是多对多通信。并且也不同于电子邮件那样一切都在用户自己的邮箱之中，用户必须使用网络新闻浏览工具访问 UseNet 主机、阅读主机的消息或发表自己的意见。

用户要想获得网络新闻，应具备两方面的条件，其一必须能访问到一台参与 UseNet 网络新闻传送的计算机，比如北京电信的网络新闻组服务器：news. bta. net. cn。其二必须安装一套新闻阅读软件，现在最为常见的软件是 Outlook Express。在 Outlook Express 中创建一个新闻账号，指定一台新闻服务器，预订感兴趣的新闻组，然后就可以阅读新闻，进行讨论了。

2.5.3 IP Phone

随着 Internet 的日益扩大，基于 IP 技术的各种应用迅速发展。其中 IP Phone 就是近几年兴起的、极具挑战性的实用技术。IP Phone 也称为网络电话、IP 电话、VoIP、Internet Telephone

等，它是建立在 Internet 基础上的新型数字化传输技术，是 IP 网上通过 TCP/IP 协议实现的一种电话应用。IP Phone 最早的产品可以追溯到 1995 年，当时开发商们推出了一些基于计算机平台的软件产品。如 Vocaltec 的 IP Phone（即 Internet Phone）、Netspeak 公司的 Web Phone，以及后来 Netscape 的 Cooltalk 等。IP Phone 可以在 Internet 上实现实时的语音传输服务，和传统电话业务相比，它具有巨大的优势和广阔的市场前景，现在，IP Phone 不仅可以提供 PC-to-PC 的实时语音通信，而且可以提供 PC-to-Phone、Phone-to-Phone 的实时语音通信，并在此基础之上还可以实现语音、视频、数据合一的实时多媒体通信。和传统的 PSTN 相比，IP Phone 具有以下优点：

（1）能够更加高效地利用网络资源。IP Phone 采用了先进的数字信号处理技术，可以将 64kbps（bit/s）的话音信号压缩成 8kbps（bit/s）或更低码率的数据流，能够在同一条线路上传输比采用模拟技术时更多的呼叫，并且 IP Phone 采用的是分组交换技术，可以实现信道的统计复用，使得网络资源的利用效率更高。

（2）可以提供更为廉价的服务。由于 IP Phone 是以数字形式作为传输媒体，所以占用资源小，成本很低，价格便宜。现在国内已经有一些电信运营商开始提供 IP Phone 服务，价格可以比传统的电话低 40％～70％。

（3）和数据业务有更大的兼容性。IP Phone 不仅包含传统的话音业务，还涵盖了其他一些多媒体实时通信业务，同时还提供了许多方便的增值业务，如呼叫转移、呼叫等候、呼叫阻塞、主叫号码显示等。

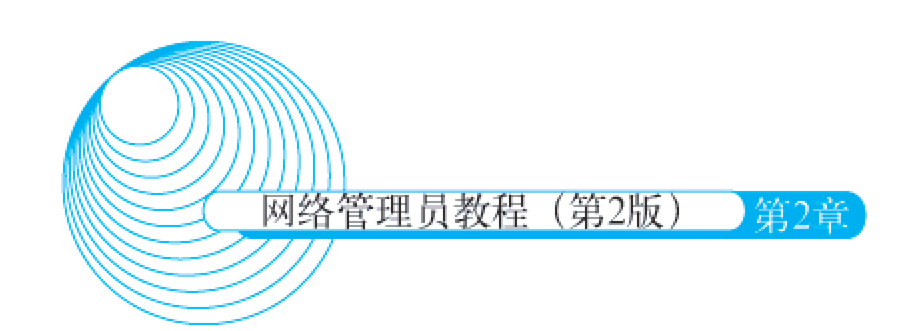
（4）符合三网合一的发展方向。IP 技术是通信领域的新潮流，它符合未来三网合一（电话网、广播电视网、数据网）的发展方向，因而其市场潜力十分可观。

IP 电话系统把来自普通电话的模拟信号转换成计算机可联入 Internet 传送的数据包，同时也将收到的数据包转换成声音的模拟电信号。IP 电话系统是由一系列组件构成的，其中包括：终端、网关、关守、网管服务器、计费服务器等。

Internet 网关提供 Internet 和电话网之间的接口，用户通过 PSTN 本地环路连接到 Internet 的网关，网关负责把模拟信号转换为数字信号并压缩打包，成为可以在 Internet 上传输的分组语音信号，然后通过 Internet 传送到被叫用户的网关端，由被叫端的网关进行分组数据的解包、解压和解码，还原为可被识别的模拟语音信号，再通过 PSTN 传到被叫方的终端。这样，就完成了一个完整的电话到电话的 IP 电话的通信过程。

2.5.4 网络娱乐

网络娱乐主要是指网络公司借助 Internet 的优势，为吸引网民参加而推出的各种娱乐活动。内容包括在线新闻竞猜、游戏、猜谜等各种娱乐。由于互动意识和参与感强，加上即时性、公开性和公平性，所以网络娱乐始终成为一大部分网民上网的主要目的。不论是国内还是国外，各



类娱乐网站在与电视和报刊的竞争中脱颖而出，迅速地吸引了大批青年网民。国外 Internet 界有关专家指出：网络生活化，生活网络化，并预言未来的人类完全可以依赖网络而生存下去了。在国内，众多 Internet 公司正在从以信息为中心转向以人为中心，而娱乐正是以人为中心的最基本体现。从目前发展来看，网络娱乐完全变成了一项产业。

网络娱乐尤其以网络游戏最具有市场和应用潜力。Internet 上所流行的网络游戏可以分为角色扮演（RPG，Role Playing Game）游戏、第一人称射击对战（FPS，First Person Shooter）游戏和泥巴（MUD，Multiple User Dimension）游戏这三大阵营。

RPG 游戏的主要特点是追求等级、收集物品、屠杀怪物，甚至是毫无道德的 PK，游戏中的人物、装备、道具、金钱等，具有现实生活中商品的最大共同特征，玩家追求的是获得使用的满足感。较有代表性的 RPG 游戏产品包括《传奇》、《仙境传说》、《天堂》、《奇迹 MU》等。同时需要指出的是，随着网络游戏的发展，网络游戏的虚拟世界与现实生活之间出现了联系通道，社会上已经出现了网络游戏代练公司，虚拟装备也出现了交易平台。现在有越来越多的人愿意将现实中的货币换成二进制的代码组合。同时，游戏运营商为延长游戏寿命，也在网络世界中不停地加入各种新式的道具和人物。

FPS 游戏的主要特点是力求真实的斗智斗勇，随着技术的不断成熟，《虚幻》、《QUAKE Ⅰ、Ⅱ、Ⅲ》、《三角洲特种部队》等各种各样的 FPS 游戏逐渐出现在游戏市场中。而《反恐精英》的诞生，更是将此类游戏提高到了一个新的层面，从单纯人与机器的对抗提高到了人与人对抗的电子竞技的时代，但这一切仍仅仅局限于局域网络之中。2002 年推出的《战地 1942》、《荣誉勋章》等二战题材的 FPS 游戏终于将玩家从单调的局域网中解放出来，FPS 游戏第一次迈入网络对战行列。

MUD 是英文 Multiple User Dimension、Multiple User Dungeon 或 Multiple User Dialogue 的缩写，可以译为多人世界、多人地下城或多人对话，俗称“泥巴”。在 MUD 中，所接触到的是一个由计算机构造出的广阔的虚拟世界，在这个世界中的每一个游戏角色背后，都有一个现实中的人在操作，他的喜怒哀乐、脾气嗜好、价值观念，无不完全投射到游戏角色身上，并影响游戏的全进程。MUD 玩家所面对的不再是计算机控制下的机器人物，而是一群有血有肉有个性，具备真正人的智慧的游戏伙伴。另一方面，这些游戏角色在 MUD 中也有其独特的人际关系和特定的行为特征（比如魔法师）。

也可以认为 MUD 是 RPG 游戏的一种。但 MUD 没有漂亮的彩色画面，通常只有一张用 ASCII 字符组成的封面，玩者只能像玩早期 RPG 一样用键盘输入文字命令。MUD 是一个环境，提供了这个虚拟世界中所有玩家扮演他们角色的舞台，玩家们可以不必像在传统 RPG 中那样按一个固定的线索发展剧情。每个人都可以在这幻想的大陆上自由行走，比传统的 RPG 更有 RPG 的味道。随着技术的进步，现在出现了 UO，即图形 MUD ，但是由于网络条件和速度的限制，文字 MUD 仍然独具它的魅力。

2.5.5 虚拟现实

1. 虚拟现实的概念

随着 Internet 的飞速发展及 3D 技术的日益成熟，人们已经不满足 Web 页上二维空间的交互特性，而希望将 WWW 变成一个立体空间。主页上将不再仅仅有图片文字，而是有三维场景，主页的链接也不再是高亮度显示的图片和文字，而是在三维空间打开一扇门或者触摸一个物体，就进入了另一个主页。甚至在网上还可以有一个虚拟的自己，上网者互相之间都能相互看到，用户可以像逛街一样浏览主页，同时和路上碰到的人打招呼，这就是虚拟现实技术的体现。

虚拟现实是从英文 Virtual Reality 一词翻译过来的，Virtual 就是虚假的意思，Reality 就是真实的意思，合并起来就是虚拟现实，也就是说本来没有的事物和环境，通过各种技术虚拟出来，让你感觉到就如真实的一样。

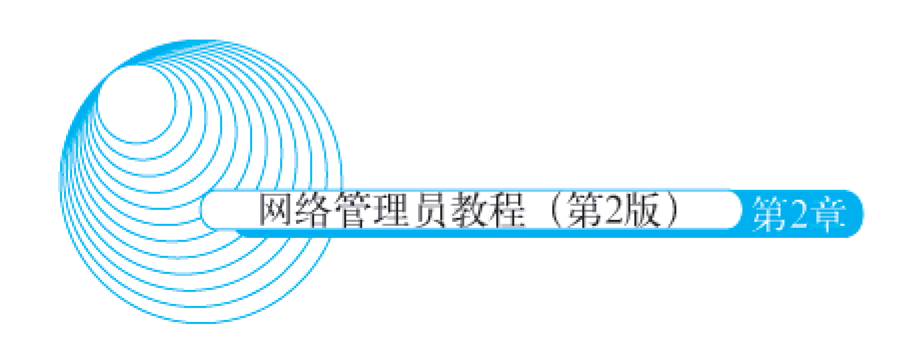
虚拟现实的定义可以归纳如下：虚拟现实是利用计算机生成一种模拟环境（如飞机驾驶舱、操作现场等），通过多种传感设备使用户"投入"到该环境中，实现用户与该环境直接进行自然交互的技术。这里所谓模拟环境就是用计算机生成的具有表面色彩的立体图形，它可以是某一特定现实世界的真实体现。也可以是纯粹构想的世界。传感设备包括立体头盔（Head Mounted Display）、数据手套（Data Glove）、数据衣（Data Suit）等穿戴于用户身上的装置和设置于现实环境中的传感装置（不直接戴在身上）。自然交互是指用日常的方式对环境内的物体进行操作（如用手拿东西、行走等）并得到实时立体反馈。

2. VRML

WWW 上的虚拟现实技术是依靠 VRML 语言来实现的，VRML 是英文 Virtual Reality Modeling Language（虚拟现实造型语言）的缩写。使用 VRML，能在 Internet 上设计三维虚拟空间。可以建造虚拟的房间、建筑物、城市、山脉和星球。能用虚拟的家具、汽车、人员、飞机或能想象出的任何东西来填充虚拟的世界。VRML 最主要的特点是，能够在 Internet 上创建动态的世界和感觉丰富的虚拟环境。在 VRML 中，可以创建锚点于 VRML 空间造型的链接。单击锚点造型将引导 VRML 浏览顺着链接检索出该链接所连的 VRML 文件。那个文件也可以包含跟踪的链接，而且以此发展下去。顺着一个 VRML 文件中的链接，用户能在 3D 空间浏览 Web，当用户漫步 Internet 时，可以从一个虚拟空间跨入另一个空间。

VRML 的基本目标是建立 Internet 上的交互式三维多媒体，基本特征包括分布式、三维、交互性、多媒体集成、境界逼真性等。

目前，Internet 上有很多 VRML 站点，使用搜索引擎就可以查到。需要说明的是，在浏览



VRML 站点前，浏览器要安装 VRML 的插件。常见的 VRML 的插件有：CosmoPlayer、blaxxun Contact、Cortona 和 WorlView 等。

3. 虚拟现实的应用

(1) 远程教育：国内外一些高等院校利用 VRML 2.0 语言，成功开发了基于集成声音、图像及其他多媒体技术的三维空间的远程教育中心，它制造了一个完全立体化的模型，虚拟出真实的校园环境，用户进入教育中心如同进入真正的学校一样，可以进行提问、考试等，进行实时的教学和交流。

(2) 商业应用：VRML 可以让顾客更好地感受想要购买的商品。对于那些期望与客户建立直接联系的公司，尤其是那些在他们的主页上向客户发送电子广告的公司，VRML 具有特别的吸引力。

(3) 网络娱乐：网络娱乐领域是 VRML 的一个重要应用领域。它能提供良好的多人之间的交互功能，提供更加逼真的虚拟环境，从而使人们能够享受其中的乐趣，带来美好的娱乐感觉。VRML 目前正朝着实时通信、大规模用户交互的方向发展。

2.5.6 电子商务

电子商务(e-Business)，是指政府、企业和个人利用计算机与网络技术实现商品买卖和资金结算的过程。电子商务是各参与方之间以电子方式而不是以物理交换或直接物理接触方式完成任何形式的业务交易。这里的电子方式包括电子数据交换(EDI)、电子支付手段、电子定货系统、电子邮件、传真、网络、电子公告系统条码、图像处理、智能卡等。一次完整的商业贸易过程是复杂的，包括交易前的商情了解、询价、报价、发送定单、应答定单、发送接收送货通知、取货凭证、支付汇兑过程等，此外还有涉及行政过程的认证等行为，涉及了资金流、物流、信息流的流动。严格地说，只有上述所有贸易过程都实现了无纸贸易，即全部是非人工介入，完全使用各种电子工具完成，才能称之为一次完整的电子商务过程。

简单地说，电子商务是在 Internet 开放的网络环境下，基于浏览器/服务器应用方式，实现消费者的网上购物、商户之间的网上交易和在线电子支付的一种新型的商业运营模式。电子商务是在虚拟空间进行的商务活动，是对传统商务活动的一次根本性革新，将使人类社会的政治和文化生活发生深刻地变革。Internet 的迅速发展使之成为继传统市场之后的又一个巨大市场，这一市场突破了国界与疆域，企业或商家可以在 Internet 上构筑覆盖全球的商业营销网，因而可以获得全球性的无限商务空间。电子商务以一种最大化网络方式将顾客、销售商、供应商和雇员联系在一起，使供需双方在最适当的时机得到最适用的市场信息，因而能够极大地促进供需双方的经济活动，减少交易费用和经营成本，提高企业经济效益和竞争能力。

通常电子商务的应用模式分为 B2B、B2C、C2C 三类。B2B(Business to Business)代表商家对

商家，B2C(Business to Citizen)代表商家对个人，C2C(Citizen to Citizen)代表个人对个人。电子商务的应用非常广泛，像网上银行、网上炒股、网上购物、网上订票、网上租赁、工资发放、费用缴纳等。

随着IT技术的迅速发展，未来的电子商务将主要以下面几种形式体现出来。

(1) EDI业务。EDI(Electronic Data Interchange)的中文意思是电子数据交换。它是电子商务发展早期的主要形式。EDI旨在票据传送的电子化。EDI在运输业中的体现是，能最大程度地利用设备、仓库获得更大效益；EDI在零售业、制造业和仓储业中的体现是，提高货物提取及周转速度，加快资金的流动；EDI在通关与报关业务中的体现是，实现货物通关自动化和国际贸易无纸化；EDI在金融保险和商检业中的体现是，能够提供快速可靠的支付，减少时间和费用，加快资金流动。

(2) 虚拟银行。随着虚拟现实技术的不断进步，银行金融业正在积极利用虚拟现实技术，创建虚拟金融世界，这也是为了适应网络商业日益发展的需要。在虚拟银行电子空间中，可以允许数以百万计的银行客户和金融客户，面向银行所提供的几十种服务，根据需要随时到虚拟银行里漫游，这些服务包括信用卡网上购物、电子货币结算、金融服务及投资业务的咨询等。虚拟银行一方面使银行能够争取到更多的顾客，并且服务成本迅速下降。另一方面也使客户能够从虚拟银行获得方便、及时、高质量的服务，同时又节省很多服务费。当前，建立网络银行最重要的是完善硬件、软件设施和完善有关技术标准和统一操作规范。

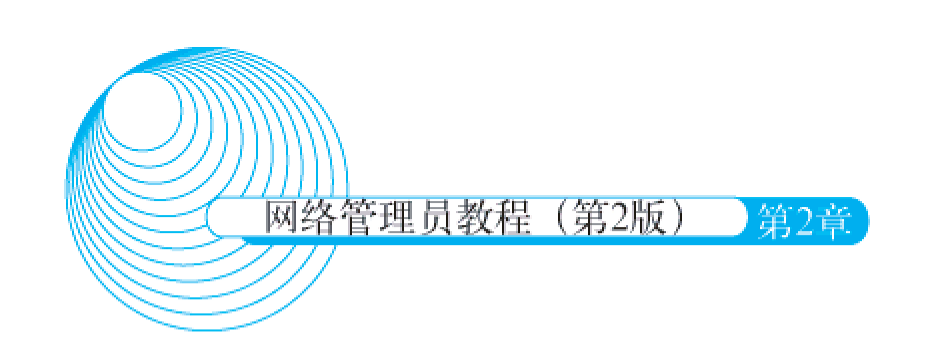
(3) 网上购物。随着电子商务技术的发展和应用，网络购物将越来越普及，并日渐成为一种新的生活时尚。网络购物利用先进的通信和计算机网络的三维图形技术，把现实的商业街搬到网上。用户无须担心出门时的天气变化，足不出户便能像真的上街那样“逛商场”，方便、省时、省力地选购商品，而且订货不受时间限制，商家会送货上门。目前在很多电子商务网站上已开通了书店、花市、电脑城、超级市场以及订票、订报、网上直销等服务。

(4) 网络广告。由于WWW提供的多媒体平台，使得通信费用降低，对于机构或公司而言，利用其进行产品宣传，非常具有诱惑力。网络广告可以根据更精细的个性差别将顾客进行分类，分别传送不同的广告信息。而且网络广告不像电视广告那样被动接受广告信息，网络广告的顾客是主动浏览广告内容的。未来的广告将利用最先进的虚拟现实界面设计达到身临其境的效果，给人们带来一种全新的感官体验。以汽车广告为例，你可以打开汽车的车门进去看一看，还可以利用计算机提供的虚拟驾驶系统体验一下驾车的感受。

2.5.7 电子政务

1. 电子政务的概念

电子政务(e-Government)即政务信息化，是指国家机关在政务活动中，全面应用现代信息技



术进行办公和管理，为社会公众提供服务。电子政务是政府机关提高行政效率、降低行政成本、形成一个“行为规范、运转有效、公正透明、廉洁高效”的行政管理体制的有效途径。

电子政务主要包括四个方面的内容：

(1) 信息发布。信息发布是指对将要公布的信息，运用 FTP 等软件上传到相应的 WWW 服务器，通过 Internet 发布给广大公众。其主要形式包括：各政府机构可以在自己的网站(包括内网和外网)上实现信息发布，并通过建立政府整体性的网络系统，进行相互间的信息传递，以增进政府之间以及政府与社会各部门之间的沟通；在各政府部门建立各种资料库的基础上，还可以通过网站进行数据库查询，向政府公务员和社会公众提供便捷的方法，使其通过 Internet 等渠道取得有关资料。

(2) 网上交互式办公。网上交互式办公是指实现在线查询、登记、申报、备案、讨论、意见征集等交互式办公，还包括政府采购、招标、审批以及网上报税和纳税等项目。网上交互式办公还体现为通过 Internet 对政府与公众之间的事务进行互动处理，能够使政府快速听到群众的呼声，对民众来信和意见做出及时处理。

(3) 内部办公自动化。内部办公自动化是指建立办公业务流程的自动化系统，从公文的拟制、审阅、签批、下发、归档，到公文的查询、借阅等全程均使用计算机网络来处理，实现电子公文。内部办公自动化还包括全程使用计算机网络处理对报表的统计、制作、汇总及管理，通过局域网进行资料信息的数据共享及交换，达到办公业务规范化、科学化和无纸化。

(4) 部门间协同工作。部门间协同工作俗称“一站式服务”，是指多个政府机构针对同一事项，利用共同的网络平台进行协同工作。

通常电子政务的应用模式分为 G2G、G2B、G2C 三类，G2G(Government to Government)代表不同的政府机构对不同的政府机构，G2B(Government to Business)代表政府机构对商家或企业，G2C(Government to Citizen)代表政府机构对公民。

2. 政府门户网站

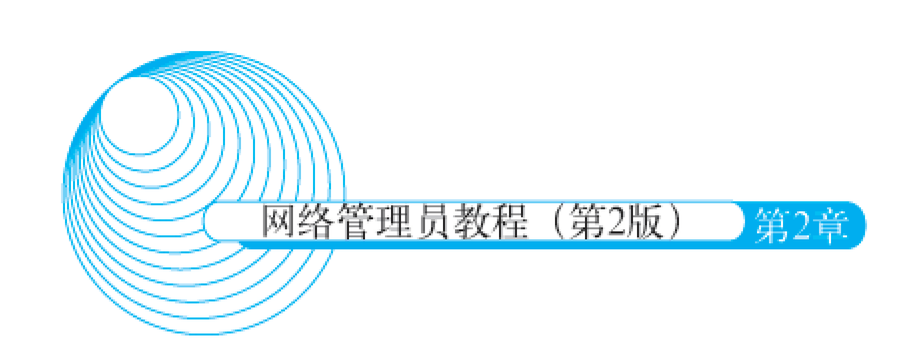
所谓政府门户网站是指在各政府部门的信息化建设基础之上，建立起跨部门的、综合的业务应用系统，使公民、企业与政府工作人员都能快速便捷地接入所有相关政府部门的业务应用、组织内容与信息，并获得个性化的服务，使相关的人能够在恰当的时间获得恰当的服务。政府门户网站作为我国电子政务建设的重要组成部分，是政府面向社会的窗口，是公众与政府互动的渠道，对于促进政务公开、推进依法行政、接受公众监督、改进行政管理、全面履行政府职能具有重要意义。不管是 G2G、G2B，还是 G2C，其应用接口都是通过政府门户网站实现的。政府门户网站不仅是政务信息发布平台和业务处理平台，而且也是知识加工平台、知识决策平台、知识获取平台的集成，它使政府各部门办公人员之间的信息共享和交流更加流畅，通过数据挖掘、数据加工而使零散的信息成为知识，使相关人员能够在恰当的时间使用恰当的知识，为行政决策

提供充分的信息和知识支持。政府门户网站有赖于各政府部门已有的信息化基础条件。后台整合是政府门户网站建设的关键所在，也就是说，实施电子政务，最重要的是其前台的业务流程设置与后台不同政府机构之间的业务协调处理。另外，正确处理政府门户网站与各政府机构内网的关系是政府门户网站建设的另一个关键所在，也就是说，在实施电子政务时，重点需要考虑的是政务内网与政务外网之间的关系，如何进行数据共享，如何架构信息安全策略等问题。

3. 我国电子政务的发展

我国电子政务的初期发展主要表现在两个方面：一是20世纪80年代末期，中央和地方党政机关所开展的办公自动化（OA）工程，建立了各种纵向和横向内部信息办公网络，为利用计算机和通信网络技术奠定了基础；二是1993年底启动的“三金工程”，即金桥工程、金关工程和金卡工程，这是中央政府主导的以政府信息化为特征的系统工程，重点是建设信息化的基础设施，为重点行业和部门传输数据和信息。但是，这些都还只是电子政务发展的雏形，是电子政务发展的初级阶段。

20世纪90年代末期，由于信息网络技术的快速发展和信息基础设施的不断完善，电子政务的发展进入快车道，突破了部门和地域限制，向交互性和Internet方向发展。1998年4月，青岛市在Internet上建立了我国第一个严格意义上的政府网站“青岛政务信息公众网”。1999年1月，40多个部委（局、办）的信息主管部门共同倡议发起了“政府上网工程”，其目标是在1999年实现60%以上的部委和各级政府部门上网，在2000年实现80%以上的部委和各级政府部门上网。1999年5月，gov.cn下注册的政府域名猛增至1470个。2002年7月3日，国家信息化领导小组颁布了《我国电子政务建设指导意见》，明确了“十五”期间我国电子政务建设的指导思想和原则，提出了在此期间我国电子政务建设的主要目标和任务以及必须采取的措施。2003年4月22日为进一步贯彻落实《我国电子政务建设指导意见》，国务院信息化工作办公室、科学技术部、信息产业部联合制定了《电子政务工程技术指南》，我国电子政务的建设逐步开始进入统一的轨道。根据CNNIC的统计，截止到2003年12月，以gov.cn为结尾注册的域名总数达到11764个。中国政府网，如图2-57所示，于2005年10月1日试开通，2006年1月1日正式开通。




中华人民共和国中央人民政府门户网站 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://www.gov.cn/
转到 链接
中文简体 | 中文繁体 | English | 邮箱 | 搜索
本网站搜索 搜索
2006年4月28日 星期五
中华人民共和国中央人民政府
The Central People's Government of the People's Republic of China
www.GOV.cn
中央政府门户网站
本网首页
今日中国
中国概况
国家机构
政府机构
法律法规
政务公开
政务互动
政府建设
工作动态
人事任免
新闻发布
网上服务
在线访谈
今日中国
中国要闻 | 领导活动 | 中外交往 | 商务之窗 | 央企在线 | 图片图表 | 视频报道
胡锦涛抵达内罗毕 同肯尼亚总统齐贝吉举行会谈 (2006-04-28)
十届全国人大常委会分组审议义务教育法修订草案 (2006-04-28)
秦山核电二期顺利通过国家竣工验收 扩建工程开工 (2006-04-28)
个人住房公积金贷款利率5月8日起上调0.18百分点 (2006-04-28)
统计局:一季度全国城镇在岗职工平均工资增长15% (2006-04-28)
交通部要求强化安全管理确保旅客黄金周出行平安 (2006-04-28)
全国假日办发布"五一"黄金周第五号旅游信息预报 (2006-04-28)
工商总局发通知要求加强"五一"期间市场监管工作 (2006-04-28)
我国自主研制的枭龙全状态飞机04架首飞圆满成功 (2006-04-28)
中国的大熊猫保护工作从人工圈养向野化放归转变 (2006-04-28)
青藏铁路建设进入最后冲刺阶段
更多图片
视频节目
热点专题
温家宝总理《政府工作报告》解读
加强卫生工作 增进人民健康 New
推进廉政工作 促进政府建设
贯彻科技大会精神 建设创新型国家
《国民经济和社会发展第十一个五年规划纲要》解读
落实科学发展观 加强环保工作 New
开展纠风工作 切实维护群众利益
迎接"两会"召开 关注惠农工作
国家重点工程 展现建设成就
2006年"五一"黄金周专题
国务院办公厅关于2006年放假通知
2006年高考服务信息
06年高油大豆春季生产技术指导意见
大陆居民赴台湾地区旅游管理办法
4月1日起一批法规规章开始实施
《机动车"强制三者险"条例》解读
设为首页 | 关于我们
应急管理
突发事件 机构设置
工作动态 应急预案
应急演练 法律法规
科普宣教 典型案例
主题服务
公民
生育 户籍 教育
文化 就业 兵役
婚姻 纳税 社保
交通 医疗 殡葬
邮政 旅游 护照
出入境 法律援助
港澳台侨
企业
开办设立 年检年审
(剩下8项) 正在打开网页 http://www.gov.cn/...
Internet

图 2-57　中国政府网

第3章 局域网技术与综合布线

3.1 局域网基础

3.1.1 局域网参考模型

1980 年 2 月，电气和电子工程师协会（IEEE，Institute of Electrical and Electronics Engineers）成立了 IEEE 802 委员会。当时个人计算机联网刚刚兴起，该委员会针对这一情况，制订了一系列局域网标准，称为 IEEE 802 标准。按照 IEEE 802 标准，局域网体系结构由物理层、媒体访问控制子层（MAC，Media Access Control）和逻辑链路控制子层 LLC（Logical Link Control）组成，如图 3-1 所示。

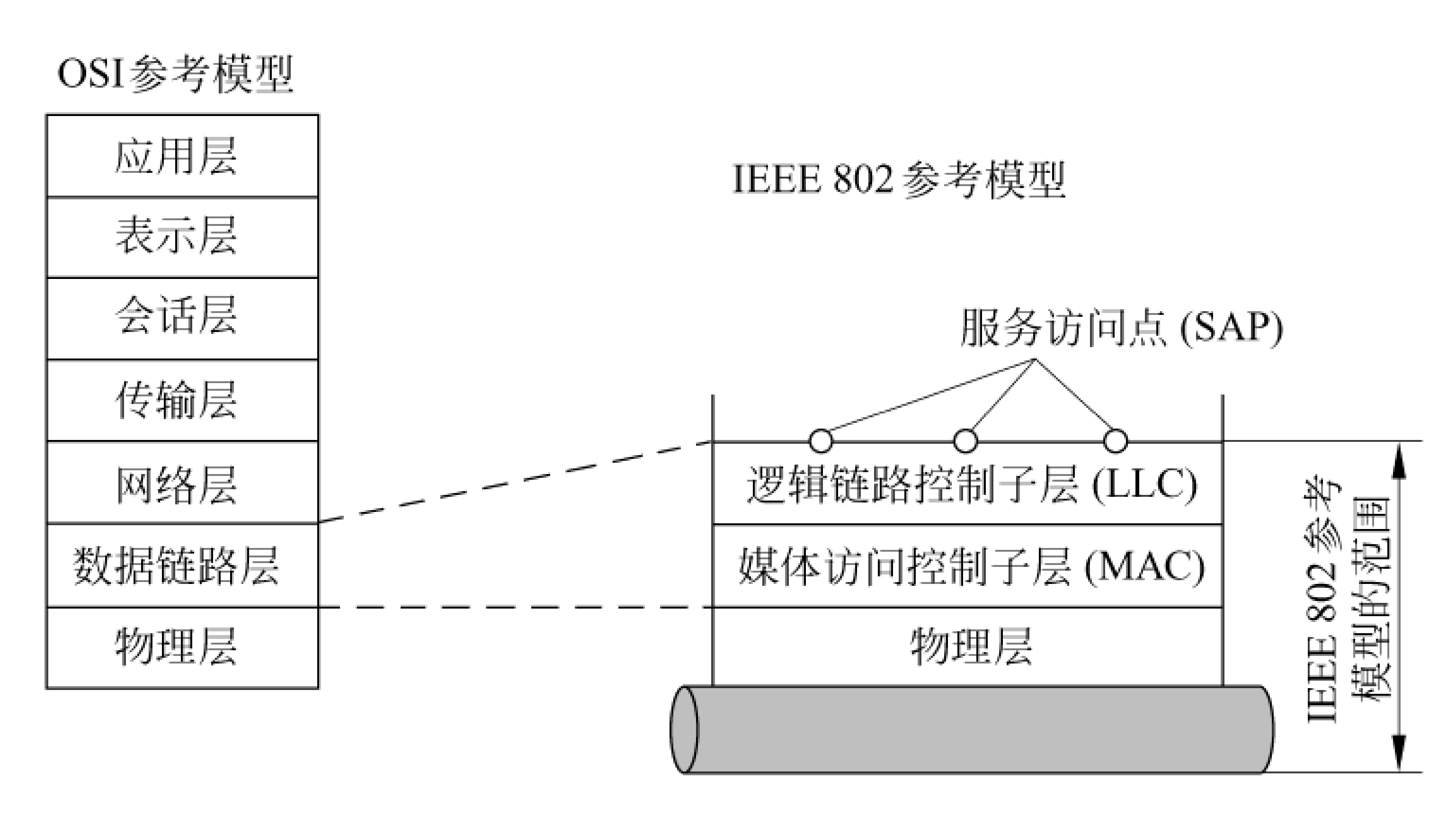


图 3-1 IEEE 802 参考模型

IEEE 802 参考模型的最低层对应于 OSI 模型中的物理层，包括以下功能：

(1) 信号的编码/解码；

(2) 前导码的生成/去除(前导码仅用于接收同步)；

(3) 比特的发送/接收。

IEEE 802 参考模型的 MAC 层和 LLC 层合起来对应 OSI 模型中的数据链路层，MAC 子层完成的功能如下：

(1) 在发送时将要发送的数据组装成帧，帧中包含有地址和差错检测等字段；

(2) 在接收时，将接收到的帧解包，进行地址识别和差错检测；

(3) 管理和控制对于局域网传输媒体的访问。

LLC 子层完成的功能如下：

(1) 为高层协议提供相应的接口，即一个或多个服务访问点(SAP，Service Access Point)，通过 SAP 支持面向连接的服务和复用能力；

(2) 端到端的差错控制和确认，保证无差错传输；

(3) 端到端的流量控制。

需要指出的是，在局域网中采用了两级寻址，用 MAC 地址标识局域网中的一个站，LLC 提供了服务访问点(SAP)地址，SAP 指定了运行于一台计算机或网络设备上的一个或多个应用进程地址。

802.10 安全与加密
802.1 局域网概述、体系结构、网络互联和网络管理
802.2 逻辑链路控制 (LLC)
LLC 层
802.3 以太网
802.4 令牌总线
802.5 令牌环
802.6 城域网
802.9 语音数据网
802.11 无线局域网
802.12 100VG AnyLAN
802.14 交互式电视网
802.15 无线蓝牙
802.16 无线城域网
802.17 电信以太网
802.20 移动宽带层
MAC 层
物理层 物理层 物理层 物理层 物理层 物理层 物理层 物理层 物理层 物理层 物理层 物理层 物理层
802.7 宽带技术
802.8 光纤技术

图 3-2　IEEE 802 参考模型各标准之间的关系

目前，由 IEEE 802 委员会制订的标准当前已近 20 个，各标准之间的关系如图 3-2 所示，具体标准如下。

- IEEE 802.1：局域网概述、体系结构、网络管理和网络互联。
- IEEE 802.2：逻辑链路控制(LLC)。
- IEEE 802.3：带碰撞检测的载波侦听多路访问(CSMA/CD)方法和物理层规范(以太网)。
- IEEE 802.4：令牌传递总线访问方法和物理层规范(Token Bus)。
- IEEE 802.5：令牌环访问方法和物理层规范(Token Ring)。
- IEEE 802.6：城域网访问方法和物理层规范分布式队列双总线网(DQDB)。
- IEEE 802.7：宽带技术咨询和物理层课题与建议实施。
- IEEE 802.8：光纤技术咨询和物理层课题。
- IEEE 802.9：综合语音/数据服务的访问方法和物理层规范。

- IEEE 802.10：互操作局域网安全标准(SILS)。
- IEEE 802.11：无线局域网(Wireless LAN)访问方法和物理层规范。
- IEEE 802.12：100VG ANY LAN 网。
- IEEE 802.14：交互式电视网(包括 Cable Modem)。
- IEEE 802.15：简单，低耗能无线连接的标准(蓝牙技术)。
- IEEE 802.16：无线城域网(MAN)标准。
- IEEE 802.17：基于弹性分组环(RPR，Resilient Packet Ring)构建新型宽带电信以太网。
- IEEE 802.20：3.5GHz 频段上的移动宽带无线接入系统。

3.1.2 局域网拓扑结构

所谓拓扑是一种研究与大小、距离无关的几何图形特性的方法。在计算机网络中，计算机作为节点，传输媒体作为连线，可构成相对位置不同的几何图形。网络拓扑结构是指用传输媒体互连各种设备的物理布局。参与 LAN 工作的各种设备用媒体互连在一起有多种方法，不同的连接方法网络的性能不同。按照不同的物理布局，局域网拓扑结构通常分为 3 种，分别是总线型拓扑结构、星型拓扑结构和环型拓扑结构。

1. 总线型拓扑结构

总线结构是使用同一媒体或电缆连接所有端用户的一种方式，也就是说，连接端用户的物理媒体由所有设备共享，如图 3-3 所示。使用这种结构必须解决的一个问题是确保端用户使用

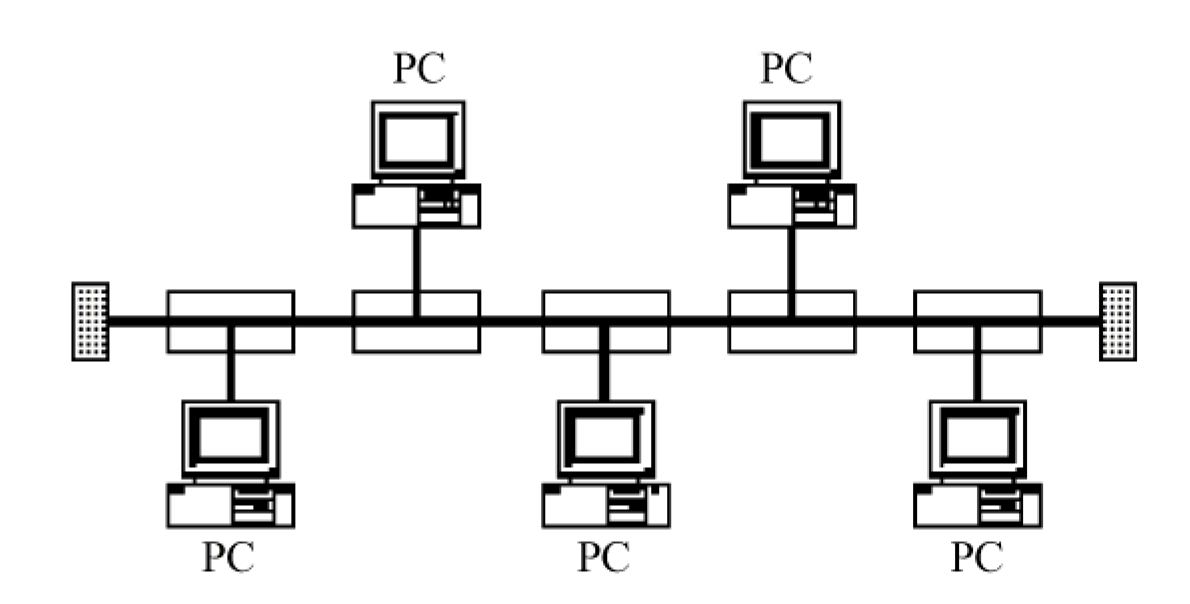


图 3-3 总线型拓扑结构

媒体发送数据时不能出现冲突。在点到点链路配置时，这是相当简单的。如果这条链路是半双工操作，只需使用很简单的机制便可保证两个端用户轮流工作。在一点到多点方式中，对线路的访问依靠控制端的探询来确定。然而，在 LAN 环境下，由于所有数据站都是平等的，不能采取上述机制。对此，研究了一种在总线共享型网络使用的媒体访问方法，即带有碰撞检测的载波侦听多路访问，英文缩写成 CSMA/CD。

这种结构具有费用低、数据端用户入网灵活、站点或某个端用户失效不影响其他站点或端用户通信的优点。缺点是一次仅能一个端用户发送数据，其他端用户必须等到获得发送权，媒体访问获取机制较复杂。尽管有上述一些缺点，但由于布线要求简单，扩充容易，端用户失效和增删不影响全网工作，所以它是LAN技术中使用最普遍的一种。

2. 星型拓扑结构

星型结构存在着中心节点，每个节点通过点对点的方式与中心节点相连，任何两个节点之间的通信都要通过中心节点来转接。图3-4为目前使用最普遍的以太网星型结构，处于中心位置的网络设备称为集线器。

这种结构便于集中控制，因为端用户之间的通信必须经过中心站。由于这一特点，也带来了易于维护和安全等优点。端用户设备因为故障而停机时也不会影响其他端用户间的通信，但这种结构非常不利的一点是，中心系统必须具有极高的可靠性，因为中心系统一旦损坏，整个系统便趋于瘫痪。对此中心系统通常采用双机热备份，以提高系统的可靠性。

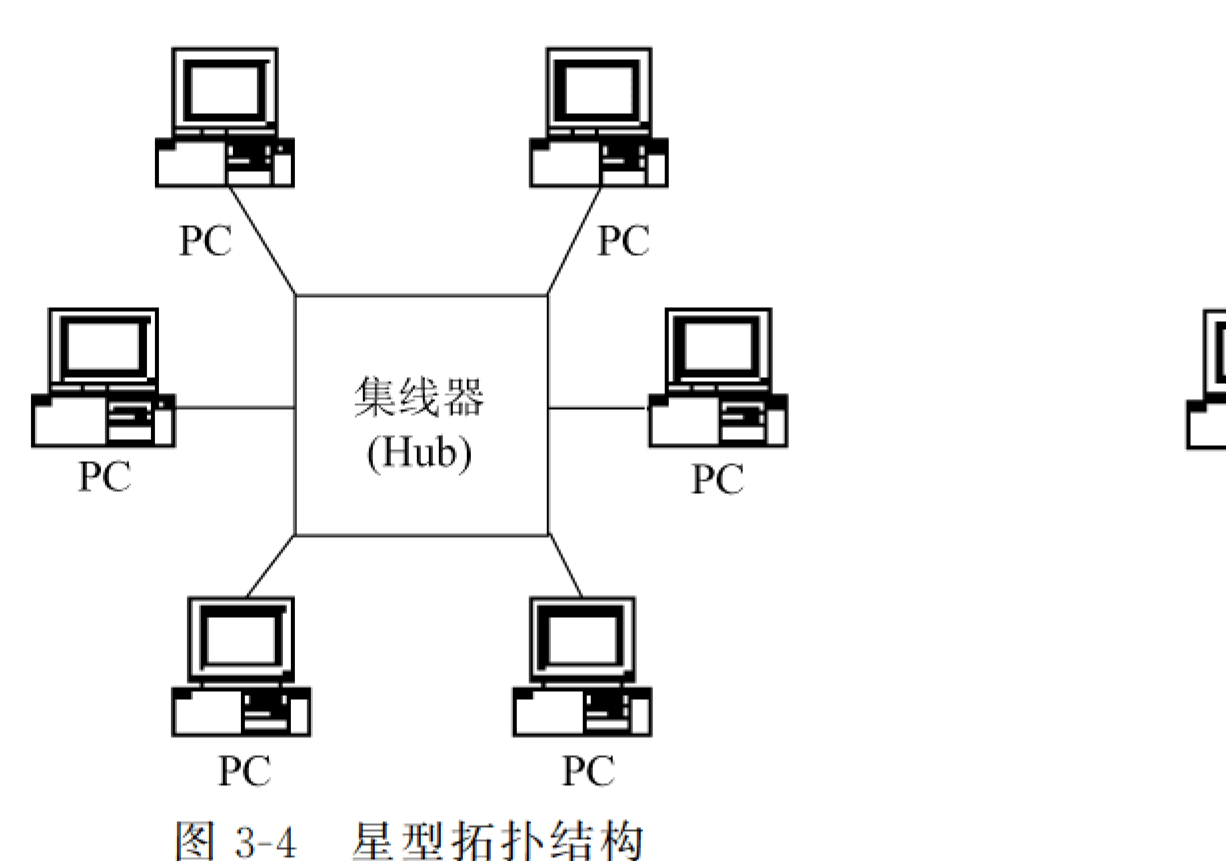
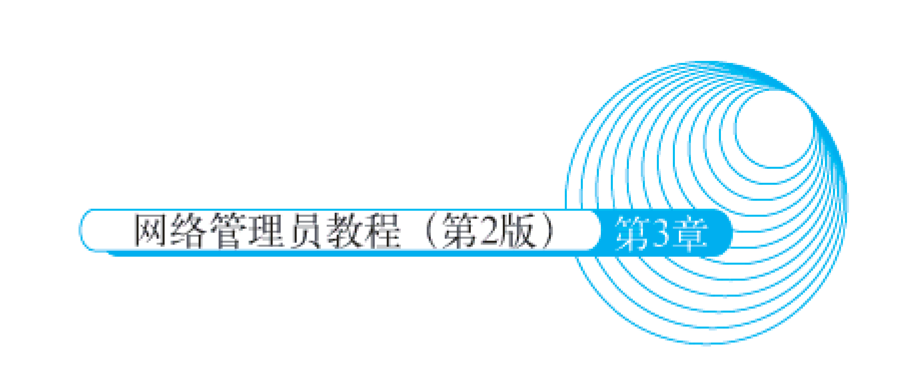


图3-4 星型拓扑结构　　图3-5 环型拓扑结构

3. 环型网络拓扑结构

环型结构在LAN中使用较多。这种结构中的传输媒体从一个端用户到另一个端用户，直到将所有端用户连成环型，如图3-5所示。这种结构显而易见消除了端用户通信时对中心系统的依赖性。

环型结构的特点是，每个端用户都与两个相邻的端用户相连，因而存在着点到点链路，构成闭合的环，但环中的数据总是沿一个方向绕环逐站传递。在环型拓扑中，多个节点共享一条环形通路，为了确定环中的节点在什么时候可以插入传送数据帧，同样要进行介质访问控制。因



此，环型拓扑的实现技术中也要解决介质访问控制方法问题。与总线型拓扑一样，环型拓扑一般也采用某种分布式控制方法，环中每个节点都要执行发送与接收控制逻辑信号。

3.1.3 局域网媒体访问控制方法

所有局域网均由共享该网络传输能力的多个设备组成。在网络中服务器和计算机众多，每台设备随时都有发送数据的需求，这就涉及到媒体的争用问题，所以需要有某些方法来控制对传输媒体的访问，以便两个特定的设备在需要时可以交换数据。传输媒体的访问控制方式与局域网的拓扑结构、工作过程有密切关系。目前，计算机局域网常用的访问控制方式有 3 种，分别是载波侦听多路访问/冲突检测（CSMA/CD）、令牌环访问控制法（Token Ring）和令牌总线访问控制法（Token Bus）。

1. 载波侦听多路访问/冲突检测（CSMA/CD）

CSMA/CD 是 Carrier Sense Multiple Access With Collision Detection 的缩写，含有两方面的内容：即载波侦听（CSMA）和冲突检测（CD）。CSMA/CD 访问控制方式主要用于总线型网络拓扑结构，是 IEEE 802.3 局域网标准的主要内容。CSMA/CD 的设计思想介绍如下。

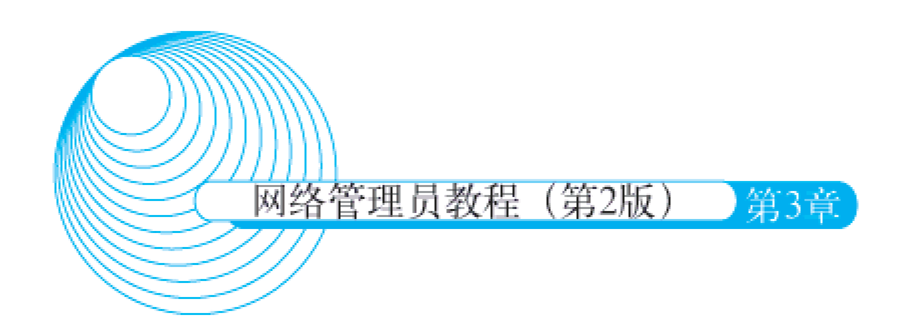
1）载波侦听多路访问（CSMA）

一个站如果要发送数据，首先要侦听（监听）总线，查看信道上是否有信号，各个站点都有一个“侦听器”，用来测试总线上有无其他工作站正在发送信息（也称为载波识别），如果信道已被占用，则此工作站等待一段时间然后再争取发送权；如果侦听总线是空闲的，没有其他工作站发送的信息就立即抢占总线进行信息发送。查看信号的有无称为载波侦听。CSMA 技术中要解决的另一个问题是侦听信道已被占用时，等待的一段时间如何确定。通常有两种方法：当某工作站检测到信道被占用后，继续侦听下去，一直等到发现信道空闲后，立即发送，这种方法称为持续的载波侦听多点访问；当某工作站检测到信道被占用后，就延迟一个随机时间，然后再检测，不断重复上述过程，直到发现信道空闲后，开始发送信息，这称为非持续的载波侦听多点访问。

2）冲突检测（CD）

当信道处于空闲时，某一个瞬间，如果总线上两个或两个以上的工作站同时都想发送数据，那么该瞬间它们都可能检测到信道是空闲的，同时都认为可以发送信息，从而一齐发送，这就产生了冲突（碰撞）；另一种情况是某站点侦听到信道是空闲的，但这种空闲可能是较远站点已经发送了信包，但由于在传输介质上信号传送的延时，信包还未传送到此站点的缘故，如果此站点又发送信息，则也将产生冲突，因此消除冲突是一个重要问题。

若在帧发送过程中检测到碰撞，则停止发送帧，形成不完整的帧（称“碎片”），在媒体上传输，并随即发送一个 Jam（强化碰撞）信号以保证让网络上所有的站都知道已出现了碰撞。发送



了 Jam 信号后，等待一段随机时间，再重新尝试发送。

在返回到重新发送帧之前，还要做以下工作。

(1) 碰撞次数 n 加 1 递增(一开始 $n=0$)；

(2) 判断碰撞次数 n 是否达到 16(十进制)；

(3) 若 $n=16$，则按"碰撞次数过多"差错处理；

(4) 若 $n<16$，则计算一个随机量 r，r 的范围为 $0<r<2k$，其中 $k=\min(n,10)$，即当$n\geq 10$，$k=10$，当 $n<10$，$k=n$；

(5) 获得延迟时间 $t=r\mathrm{T}$。

其中，T 为常数，是网络上固有的一个参数，称为"碰撞槽时间"(slot time)。延迟时间 t 又称"退避时间"，它表示检测到碰撞后要重新发送帧需要一段随机延迟时间，以错开发生碰撞各站的重新发送帧的时间。这种规则又称为"截短二进制指数退避"(Truncated Binary Exponential Backoff)规则，即退避时间是碰撞时间的 r 倍。

3) 碰撞槽时间

slot time 即是在帧发送过程中，发生碰撞时间的上限。即在这段时间中，可能检测到碰撞，而一过这段时间，永远不会发生碰撞，当然也不会检测到碰撞。也就是说，当发送的帧在媒体上传播时，超过了 slot time 后，再也不会发生碰撞，直到发送成功，或者说，一过这段时间，发送站争用媒体成功。

为了理解 slot time，并进一步了解该参数的重要性，先分析检测一次碰撞需要多长时间，如图 3-6 所示，假设公共总线媒体长度为 S，A 与 B 两个站点分别配置在媒体的两个端点上(即 A 与 B 站相距 S)，帧在媒体上传播速度为 0.7C(C 为光速)，网络的传输率为 R(b/s)，帧长为 L(bit)。

图(a)表示 A 站正开始发送帧 f_A，沿着媒体向 B 站传播；图(b)表示 f_A 快到 B 站前一瞬间，B 站发送帧 f_B；图(c)表示了在 B 站处发生了碰撞，B 站立即检测到碰撞，同时碰撞信号沿媒体向 A 站回传；图(d)表示碰撞信号返回到 A 站，此时 A 站的 f_A 尚未发送完毕，因此 A 站能检测到碰撞。

从上面 f_A 发送后直到 A 站检测到碰撞为止，这段时间间隔就是 A 站能够检测到碰撞的最长时间，这段时间一过，网络上不可能发生碰撞，slot time 的物理意义就是这样描述的，近似地可以用以下公式表示：

$$\text{slot time} \approx 2S/0.7C + 2t_{PHY}$$

其中 C 为光速，0.7C 是信号在媒体上的传输速度，t_{PHY}为 A 站物理层的延时，因为发送帧和检测碰撞都在 MAC 层中进行，因此必须要加上 2 倍的物理层延时时间。

A 站为了在 slot time 上检测到碰撞，它至少要发送的帧长 L_{min}由以下公式表示：

$$L_{min}/R = \text{slot time}$$

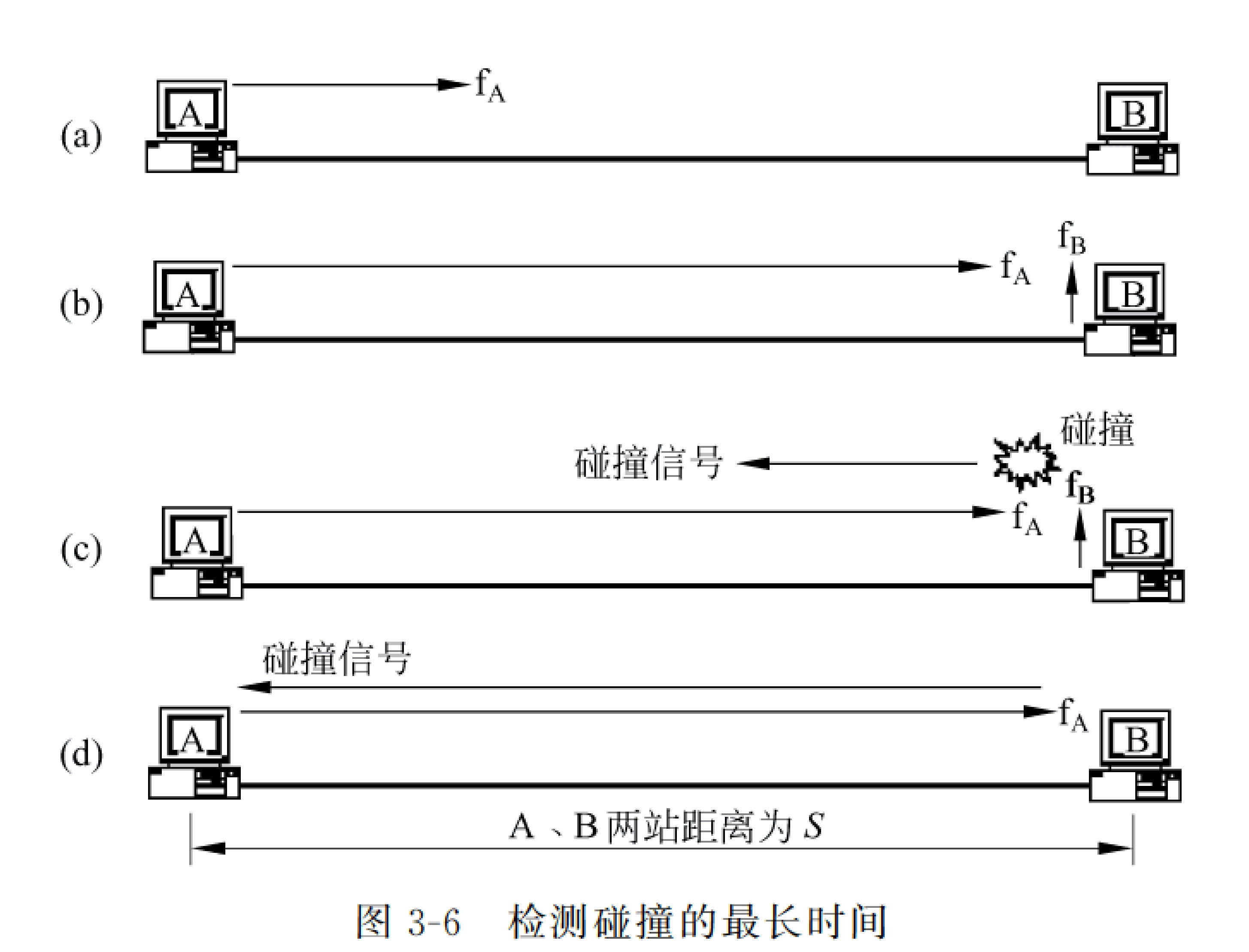


图 3-6 检测碰撞的最长时间

$$L_{min} \approx (2S/0.7C + 2t_{PHY}) \times R$$

L_{min}称为最小帧长度，由于碰撞只可能发生在小于或等于 L_{min} 范围内，因此 L_{min} 也可理解为媒体上传播的最大帧碎片长度。

综上所述，slot time 是 CSMA/CD 机理中一个极为重要的参数，这一参数描述了在发送帧的过程中处理碰撞的 4 个方面：

（1）它是检测一次碰撞所需的最长时间。即超过了该时间，媒体上的帧再也不会遭到碰撞而损坏。

（2）必须要求发送的帧长度有个下限限制，即所谓“最小帧长度”。最小帧长度能保证在网络最大跨距范围内，任何站在发送帧后，若碰撞产生，都能检测到。因为任何站要检测到碰撞必须在帧发送完毕之前，否则碰撞产生后，可能漏检，造成传输错误。

（3）它是在碰撞产生后，决定了在媒体上出现的最大帧碎片长度。

（4）作为碰撞后帧要重新发送所需的时间延迟计算的基准。

从公式 $L_{min} \approx (2S/0.7C + 2t_{PHY}) \times R$ 可以知道，光速 C 和物理层延时 t_{PHY} 是常数，对于一个具有 CSMA/CD 的公共总线（或树型）拓扑结构的局域网来说，公式中其他 3 个参数 L_{min}、S 及 R 作为变量互为正、反比关系。例如，当传输率 R 固定时，最小帧长度与网络跨距具有正比的关系，即跨距越大时，L_{min} 越长；当 L_{min} 不变的情况下，传输率越高，跨距 S 越小。这些分析对以太网的性能和发展以及高速以太网的特点均有指导性意义。

4）接收规则

在以太网结构中，节点的发送是需要通过竞争获得总线的使用权，而其他节点都应处于接收状态。当一个节点完成一组数据接收后，首先要判断接收帧的长度。因为 IEEE 802.3 协议

对帧的最小长度做了规定。凡接收帧长度小于规定帧的最小长度必然是冲突后的废弃帧。因此，如果帧太短，则表明冲突发生，接收节点丢弃已接收数据，并重新进入等待接收状态。如果说没有发生冲突，接收节点检查帧目的地址。如果目的地址为单一节点的物理地址，并且是本节点地址，则接收该帧。如目的地址是组地址，而接收节点属于该组，则接收该帧。如目的地址是广播地址，也应接收该帧。否则丢弃该接收帧。

如果接收节点进行地址匹配后，确认应接收该帧，则下一步应进行 CRC 校验。如果 CRC 校验正确，进一步应检查 LLC 数据长度是否正确。如 LLC 数据长度正确，则 MAC 子层将帧中 LLC 数据送 LLC 子层，进入"成功接收"的结束状态。如果说 LLC 数据长度不对，则进入"帧长度错"的结束状态。如果帧校验中发现错误，首先应判断接收帧是不是 8bit 的整数倍。如果帧是 8bit 的整数倍，表示传输过程中没有发现比特丢失或对位错，此时应进入"帧校验错"结束状态；如果帧长度不是 8bit 的整数倍，则进入"帧比特错"结束状态。

从以上讲解中可以看出，任何一个节点发送数据都要通过 CSMA/CD 方法去争取总线使用权，从它准备发送到成功发送的发送等待延迟时间是不确定的。因此人们将以太网所使用的 CSMA/CD 方法定义为一种随机争用型介质访问控制方法。

CSMA/CD 方式的主要特点是：原理比较简单，技术上较易实现，网络中各工作站处于同等地位，不需要集中控制，但这种方式不能提供优先级控制，各节点争用总线，不能满足远程控制所需要的确定延时和绝对可靠性的要求。另外，此方式效率高，但当负载增大时，发送信息的等待时间较长。

2. 令牌环访问控制法（Token Ring）

Token Ring 是令牌通行环（Token Passing Ring）的简写。其主要技术指标是：网络拓扑为环形布局，基带网，数据传送速率 4Mbps，采用单个令牌（或双令牌）的令牌传递方法。环型网络的主要特点是：只有一条环路，信息单向沿环流动，无路径选择问题。

令牌环技术的基础是使用了一个称之为令牌的特定比特串，当环上所有的站都处于空闲时，令牌沿环传递。当某一站想发送帧时必须等待，直至检测到经过该站的令牌为止。这时该站改变令牌中的一个比特，从而抓住令牌，然后将令牌加在发送数据帧的帧首，变成发送数据帧。此时在环上不再有令牌，因此其他想发送帧的站必须等待。这个发送数据帧将在环上环行一周，然后由发送站将其清除。发送站在下列两个条件都符合时，将在环上释放一个新的令牌：

（1）本站已完成帧的发送；

（2）本站所发送帧的前沿已回到本站（帧已绕环运行一整圈）。

其他站在环上监听，并不断地转发着经过的帧。每个站都能对经过的帧进行检测，如果检测到的目的地址是本身的地址，并且本站有足够的缓存，就复制该帧，从而达到了接收的目的。同时，继续转发该信息包。环上的帧信息绕网一周，由源发送点予以收回。按这种方式工作，发

送权一直在源站点控制之下，只有发送信包的源站点放弃发送权，把 Token 置“空”后，其他站点得到令牌才有机会发送自己的信息。

令牌方式在轻负载时，由于发送信息之前必须等待令牌，加上规定由源站收回信息，大约有50%的环路在传送无用信息，所以效率较低。然而在重负载环路中，令牌以“循环”方式工作，故效率较高，各站机会均等。令牌环的主要优点在于它提供的访问方式的可调整性，它可提供优先权服务，具有很强的实时性。其主要缺点是有令牌维护要求，为避免令牌丢失或令牌重复，导致这种方式的控制电路较复杂。

3. 令牌总线访问控制法(Token Bus)

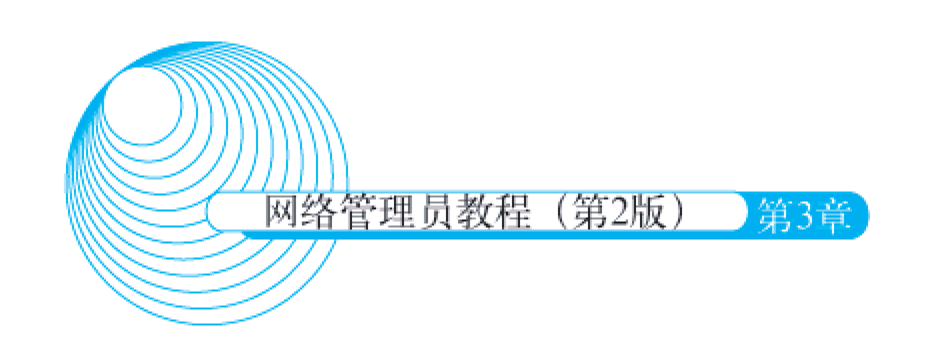
Token Bus 是令牌通行总线(Token Passing Bus)的简写。这种方式主要用于总线型或树型网络结构中。1976 年美国 Data Point 公司研制成功的 ARCnet(Attached Resource Computer)网络，它综合了令牌传递方式和总线网络的优点，在物理总线结构中实现令牌传递控制方法从而构成一个逻辑环路。此方式也是目前微机局域网中的主流介质访问控制方式。

ARCnet 网络就是将总线或树型传输介质上的各工作站形成一个逻辑上的环，即将各工作站置于一个顺序的序列内(例如可按照接口地址的大小排列)。方法可以是在每个站点中设一个网络节点标识寄存器 NID，初始地址为本站点地址。网络工作前，要对系统初始化，以形成逻辑环路，其过程主要是：网中最大站号 n 开始向其后继站发送“令牌”信包，目的站号为 $n+1$，若在规定时间内收到肯定的信号 ACK，则 $n+1$ 站连入环路，否则再加 1，继续向下询问(该网中最大站号为 $n=255$，$n+1$ 后变为 0，然后按 1、2、3、…递增)，凡是给予肯定回答的站都可连入环路并将给予肯定回答的后继站号放入本站的 NID 中，从而形成了一个封闭逻辑环路，经过一遍轮询过程，网络各站标识寄存器 NID 中存放的都是其相邻的下游站地址。

逻辑环形成后，令牌的控制方法类似于 Token Ring。在 Token Bus 中，信息是按双向传送的，每个站点都可以“听到”其他站点发出的信息，所以令牌传递时都要加上目的地址，明确指出下一个控制站点。这种方式与 CSMA/CD 方式的不同在于除了当时得到令牌的工作站之外，其余所有的工作站只收不发，只有当收到令牌后才能开始发送，所以拓扑结构虽然是总线型结构但可以避免冲突。

Token Bus 方式的最大优点是具有极好的吞吐能力，且吞吐量随数据传输速率的增高而增加并随介质的饱和而稳定下来但并不下降；各工作站不需要检测冲突，故信号电压允许较大的动态范围，连网距离较远；有一定实时性，在工业控制中得到了广泛应用，如 MAP 网就是用的宽带令牌总线。其主要缺点在于其复杂性和时间开销较大，工作站可能必须等待多次无效的令牌传送后才能获得令牌。

应该指出，ARCnet 网实际上采用称为集中器的硬件联网，物理拓扑上有星型和总线型两种连接方式。



3.1.4 无线局域网简介

21世纪的网络已经渗透到了个人、企业以及政府。现在的网络建设已经发展到无所不在，在任何时间、任何地点都可以轻松上网。网络无所不在其实并不简单，光靠光纤、铜缆是不够的，毕竟在许多场合不允许铺设线缆。因此，需要推广一种新的解决方案，使得网络的无所不在能够得以实现，这种解决方案就是无线数据网。

1. 无线数据网络种类

无线数据网络解决方案包括：无线个人网、无线局域网、无线城域网和无线广域网。

（1）无线个人网（WPAN，Wireless Personal Area Network）：主要用于个人用户工作空间，典型距离覆盖几米，可以与计算机同步传输文件，访问本地外围设备，如打印机等。WPAN通常形象描述为“最后10米”的通信需求，目前主要技术为蓝牙（Bluetooth）。

蓝牙技术源于1994年Ericsson提出的无线连线与个人接入的想法。1997年Ericsson、IBM、Intel、Nokia和Toshiba这几个公司商议建立一种全球化的无线通信个人接入与无线连线新手段，定名为“蓝牙”（Bluetooth）。Bluetooth是一位在10世纪统一了丹麦和挪威的丹麦国王。发明者无疑希望蓝牙技术也能够像这位国王一样，把移动电话、笔记本电脑和手持设备紧密地结合在一起。1998年5月正式发起成立了“蓝牙特别兴趣组织”（BSIG，Bluetooth Special Interest Group），简称蓝牙SIG。同期，1998年3月在IEEE 802.11项目组中，对WPAN感兴趣的人士成立了研究小组，命名为IEEE 802.15工作组，主要工作是在WPAN内对无线媒体接入控制（MAC）和物理层（PHY）进行规范。为了保持两个标准的互操作性，蓝牙SIG采纳了WPAN的标准，即IEEE 802.15标准。这样蓝牙1.0版本达到与IEEE 802.15之间100%的互操作性。

1999年11月Motorola、Lucent、Microsoft及3Com加盟BSIG，成为BSIG的9个发起成员，使蓝牙技术的发展获得了更强有力的支持，并显示出更明朗的前景。现今，BSIG的参加成员已达2500多个，其发展势头令人瞩目。目前蓝牙信道带宽为1MHz，异步非对称连接最高数据速率723.2kbps；连接距离多半为10m左右。为了适应未来宽带多媒体业务需求，蓝牙速率亦拟进一步增强，新的蓝牙标准2.0版拟支持高达10Mbps以上速率（4Mbps、8Mbps、12Mbps、20Mbps）。

（2）无线局域网（WLAN，Wireless LAN）：WLAN顾名思义是一种借助无线技术取代以往有线布线方式构成局域网的新手段。WLAN可提供传统有线局域网的所有功能，是计算机网络与无线通信技术相结合的产物。WLAN利用射频无线电或红外线，借助直接序列扩频或跳频扩频、GMSK、OFDM等技术，甚至将来的超宽带传输技术UWBT，实现固定、半移动及移动的网络终端对因特网进行较远距离的高速连接访问，支持的传输速率从2Mbps到54Mbps。WLAN通

常形象描述为“最后 100 米”的通信需求，如企业网和驻地网等。

1997 年 6 月，IEEE 推出了 IEEE 802.11 标准，开创了 WLAN 先河。目前，WLAN 领域主要是 IEEE 802.11x 系列。IEEE 802.11 是 IEEE 于 1997 年最初制订的一个 WLAN 标准。主要用于解决办公室无线局域网和校园网中用户终端的无线接入，其业务范畴主要限于数据存取，速率最高只能达 2Mbps。由于它在速率、传输距离、安全性、电磁兼容能力及服务质量方面均不尽如人意，从而产生了其系列标准，IEEE 802.11x 系列标准中应用最广泛的是 IEEE 802.11b。IEEE 802.11b 将速率扩充至 11Mbps，并可在 5.5Mbps、2Mbps 及 1Mbps 之间进行自动速率调整，亦提供了 MAC 层的访问控制和加密机制，从而达到了与有线网络相同级别的安全保护，还提供了可供选择的 40 位及 128 位的共享密钥算法，从而成为目前 IEEE 802.11 系列的主流产品。而 IEEE 802.11b+ 还可将速率增强至 22Mbps。IEEE 802.11a 工作在 5GHz 频带，数据传输速率将提升到 54Mbps。

目前，IEEE 802.11 系列得到了许多半导体器件制造商的支持，这些制造商成立了一个无线保真联盟 Wi-Fi(Wireless Fidelity)。Wi-Fi 实质上是一种商业认证，表明具有 Wi-Fi 认证的产品要符合 IEEE 802.11 无线网络规范。无疑，Wi-Fi 为 IEEE 802.11 标准的推广起到了积极的促进作用。

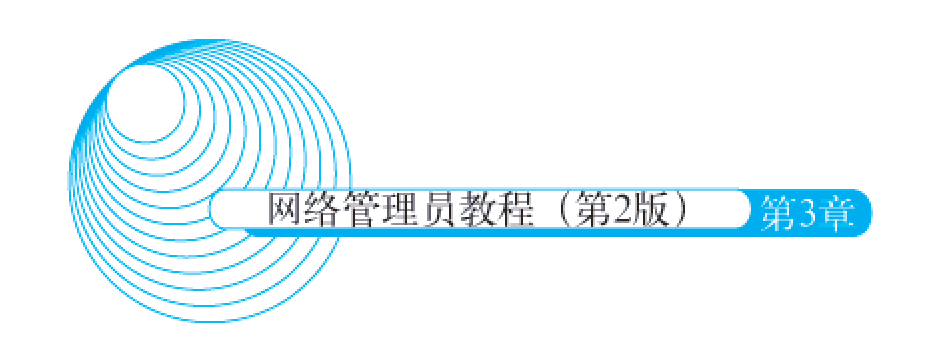
(3) 无线城域网(WMAN，Wireless MAN)：WMAN 是一种有效作用距离比 WLAN 更远的宽带无线接入网络，通常用于城市范围内的业务点和信息汇聚点之间的信息交流和网际接入。有效覆盖区域为 2～10km，最大可达 30km，数据传输速率最快可高达 70Mbps。目前主要技术为 IEEE 802.16 系列。

IEEE 802.16 标准于 2001 年 12 月获得批准，其主题为 Air Interface For Fixed Broadband Wireless Access System，即“宽带固定无线接入系统的空中接口”。标准对无线接入设备的媒体接入控制层和物理层制订了技术规范。IEEE 802.16 标准可支持 1GHz 到 2GHz、10GHz，以及 12GHz 到 66GHz 等多个无线频段。

借鉴 Wi-Fi 模式，一个同样由多个顶级制造商组成的全球微波接入互操作联盟(WiMax，Wireless Interoperability Microwave Access)宣告成立。WiMax 的目标是帮助推动和认证采用 IEEE 802.16 标准的器件和设备具有兼容性和互操作性，促进这些设备的市场推广。

(4) 无线广域网(WWAN，Wireless WAN)：无线广域网主要是解决超出一个城市范围的信息交流无线接入需求的。IEEE 802.20 和 3G 蜂窝移动通信系统构成了 WWAN 的标准。

2002 年 11 月，IEEE 802 标准委员会成立了 IEEE 802.20 工作组，即移动宽带无线接入(MBWA，Mobile Broadband Wireless Access)工作组，其主要任务是制订适用于各种工作在 3.5GHz频段上的移动宽带无线接入系统公共空中接口的物理层和媒体访问控制层的标准协议。这个标准初步规划是为以 250km/h 速度前进的移动用户提供高达 1Mbps 的高带宽数据传输，这将为高速移动用户创造使用视频会议等对带宽和时间敏感的应用的条件。拟议中的



IEEE 802.20 标准的覆盖范围同现在的移动电话系统一样，都是全球范围的，而传输速度却达到了 Wi-Fi 水平，与现在的移动通信网络相比具有明显的优势。

ITU 早在 1985 年就提出工作在 2GHz 频段的移动商用系统为第三代移动通信系统，国际上统称为 IMT-2000 系统（International Mobile Telecommunications-2000），简称 3G（3rd Generation）。ITU 所设定的 3G 标准的主要特征包括：国际统一频段、统一标准；实现全球的无缝漫游；提供更高的频谱效率，更大的系统容量，是目前 2G 技术的 2～5 倍；提供移动多媒体业务。其设计目标为：高速移动环境支持 144kbps，步行慢速移动环境支持 384kpbs，室内环境下支持 2Mbps 的数据传输，从而为用户提供包括话音、数据及多媒体等在内的多种业务。3G 的 3 大主流无线接口标准分别是 W-CDMA、CDMA2000 和 TDS-CDMA。其中 W-CDMA 标准主要起源于欧洲和日本，CDMA2000 系统主要是由美国高通北美公司为主导提出的，时分同步码分多址接入标准 TD-SCDMA 由中国提出，并在此无线传输技术（RTT）的基础上与国际合作，完成了 TD-SCDMA 标准，成为 CDMA TDD 标准的一员，这是中国移动通信界的一次创举，也是中国对第三代移动通信发展的贡献。在与欧洲、美国各自提出的 3G 标准的竞争中，中国提出的 TD-SCDMA 已正式成为全球 3G 标准之一，这标志着中国在移动通信领域已经进入世界领先之列。

2. 无线局域网扩频技术

无线局域网采用电磁波作为载体传送数据信息。对电磁波的使用有两种常见模式：窄带和扩频。窄带微波（Narrowband Microwave）技术，适用于长距离点到点的应用，可以达到 40km，最大带宽可达 10Mbps，但受环境干扰较大，不适合用来进行局域网数据传输。所以目前无线局域网的数据传输通常采用无线扩频技术 SST（Spread Spectrum）。

常见的扩频技术包括两种：跳频扩频（FHSS，Frequency-Hopping Spread Spectrum）和直接序列扩频（DSSS，Direct Sequence Spread Spectrum），它们工作在 2.4～2.4835GHz。这个频段称为 ISM 频段（Industrial Scientific Medical Band），主要开放给工业、科学、医学 3 方面使用，该频段是依据美国联邦通信委员会（FCC）定义出来的，在美国，属于免执照（Free License），并没有使用授权的限制。

跳频技术将 83.5MHz 的频带划分成 79 个子频道，每个频道带宽为 1MHz。信号传输时在 79 个子频道间跳变，因此传输方与接收方必须同步，获得相同的跳变格式，否则，接收方无法恢复正确的信息。跳频过程中如果遇到某个频道存在干扰，将绕过该频道。受跳变的时间间隔和重传数据包的影响，跳频技术的典型带宽限制为 2～3Mbps。无线个人网采用的蓝牙技术就是采用跳频技术，该技术提供非对称数据传输，一个方向速率为 720kbps，另一个方向速率仅为 57kbps。蓝牙技术也可以传送 3 路双向 64kbps 的话音。

直接序列扩频技术是无线局域网 IEEE 802.11b 采用的技术，将 83.5MHz 的频带划分成 14 个子频道，每个频道带宽为 22MHz。直接序列扩频技术用一个冗余的位格式来表示一个数据

位，这个冗余的位格式称为 chip，因此它可以抗拒窄带和宽带噪音的干扰，提供更高的传输速率。直接序列扩频技术(DSSS)提供的最高带宽为 11Mbps，并且可以根据环境因素的限制自动降速至 5.5Mbps、2Mbps、1Mbps。

3. 无线局域网拓扑结构

无线局域网组网分两种拓扑结构：对等网络和结构化网络。

(1) 对等网络(Peer to Peer)用于一台计算机(无线工作站)和另一台或多台计算机(其他无线工作站)的直接通信，该网络无法接入有线网络中，只能独立使用。对等网络中的一个节点必须能“看”到网络中的其他节点，否则就认为网络中断，因此对等网络只能用于少数用户的组网环境，比如 4～8 个用户，并且他们离得足够近。

(2) 结构化网络(Infrastructure)由无线访问点 AP(Access Point)、无线工作站 STA(Station)以及分布式系统(DSS)构成，覆盖的区域分基本服务区(BSS，Basic Service Set)和扩展服务区(ESS，Extended Service Set)。

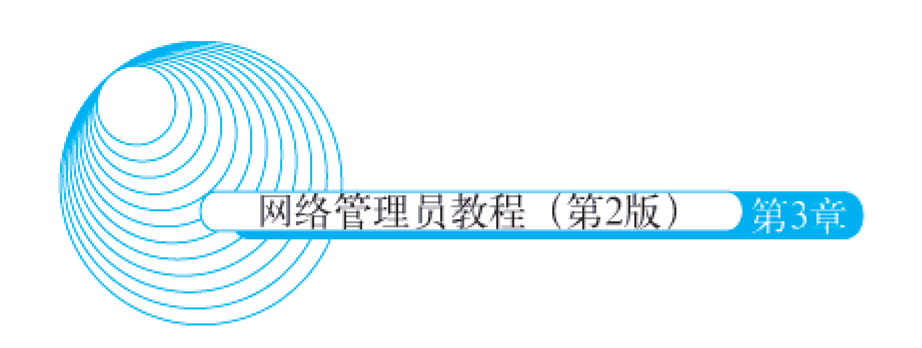
无线访问点也称无线集线器，用于在无线工作站(STA)和有线网络之间接收、缓存和转发数据。无线访问点通常能够覆盖几十至几百用户，覆盖半径达上百米。基本服务区由一个无线访问点以及与其关联的无线工作站构成，在任何时候，任何无线工作站都与该无线访问点关联。一个无线访问点所覆盖的微蜂窝区域就是基本服务区。无线工作站与无线访问点关联采用 AP 的基本服务区标识符(BSSID)，在 IEEE 802.11 中，BSSID 是 AP 的 MAC 地址。扩展服务区是指由多个 AP 以及连接它们的分布式系统组成的结构化网络，所有 AP 必须共享同一个扩展服务区标识符(ESSID)，也可以说扩展服务区 ESS 中包含多个 BSS。

无线局域网产品中的楼到楼网桥(Building to Building Bridge)为难以布线的场点提供了可靠的、高性能的网络连接。使用无线楼到楼网桥可以得到高速度、长距离的连接。事实上，可以得到超过两路 T1 线路的流量。无线楼到楼网桥可以提供点到点、点到多点的连接方式，用户可以选择最符合需求的天线：传输近距离的全向性天线，或传输远距离的扇型指向性天线。

4. 无线局域网的几个主要工作过程

(1) 扫频：STA 在加入服务区之前要查找哪个频道有数据信号，分主动和被动两种方式。主动扫频是指 STA 启动或关联成功后扫描所有频道；一次扫描中，STA 采用一组频道作为扫描范围，如果发现某个频道空闲，就广播带有 ESSID 的探测信号；AP 根据该信号做响应。被动扫频是指 AP 每 100ms 向外传送灯塔信号，包括用于 STA 同步的时间戳，支持速率以及其他信息，STA 接收到灯塔信号后启动关联过程。

(2) 关联(Associate)：用于建立无线访问点和无线工作站之间的映射关系，实际上是把无线变成有线网的连线。分布式系统将该映射关系分发给扩展服务区中的所有 AP。一个无线工作



站同时只能与一个 AP 关联。在关联过程中，无线工作站与 AP 之间要根据信号的强弱协商速率，速率变化包括 11Mbps、5.5Mbps、2Mbps 和 1Mbps。

(3) 重关联(Reassociate)：就是当无线工作站从一个扩展服务区中的一个基本服务区移动到另外一个基本服务区时，与新的 AP 关联的整个过程。重关联总是由移动无线工作站发起。

(4) 漫游(Roaming)：指无线工作站在一组无线访问点之间移动，并提供对于用户透明的无缝连接，包括基本漫游和扩展漫游。基本漫游是指无线 STA 的移动仅局限在一个扩展服务区内部。扩展漫游是指无线 SAT 从一个扩展服务区中的一个 BSS 移动到另一个扩展服务区的一个 BSS，IEEE 802.11 并不保证这种漫游的上层连接。常见做法是采用 Mobile IP 或动态 DHCP。

5. 无线局域网的访问控制方式

已经知道 IEEE 802.3 标准的以太网使用 CSMA/CD 的访问控制方法。在这种介质访问机制下，准备传输数据的设备首先检查载波通道。如果在一定时间内没有侦听到载波，那么这个设备就可以发送数据。如果两个设备同时发送数据，冲突就会发生，并被所有冲突设备所检测到。这种冲突便延缓了这些设备的重传，使得它们在间隔某一随机时间后才发送数据。而 IEEE 802.11b 标准的无线局域网使用的是带冲突避免的载波侦听多路访问方法(CSMA/CA)。冲突检测(Collision Detection)变成了冲突避免(Collision Avoidance)，这一字之差是很大的。因为在无线传输中侦听载波及冲突检测都是不可靠的，侦听载波有困难。另外通常无线电波经天线送出去时，自己是无法监视到的，因此冲突检测实质上也做不到。在 IEEE 802.11 中侦听载波是由两种方式来实现，一个是实际去听是否有电波在传，然后加上优先权控制。另一个是虚拟的侦听载波，告知等待多久的时间要传东西，以防止冲突。

CSMA/CA 通信方式将时间域的划分与帧格式紧密联系起来，保证某一时刻只有一个站点发送，实现了网络系统的集中控制。因传输介质不同，CSMA/CD 与 CSMA/CA 的检测方式也不同。CSMA/CD 通过电缆中电压的变化来检测，当数据发生碰撞时，电缆中的电压就会随之发生变化；而 CSMA/CA 采用能量检测(ED)、载波检测(CS)和能量载波混合检测 3 种检测信道空闲的方式。

3.2 以太网

3.2.1 以太网简介

今天大家熟知的以太网(Ethernet)是 Xerox 公司在 1972 年开创的。在 1972 年秋，一位刚从麻省理工学院毕业的学生 Bob Metcalfe 来到 Xerox palo Alto 研究中心(PARC)计算机实验室工作，Metcalfe 的第一件工作是把 Xerox ALTO 计算机连到 ARPANet 上(ARPANet 是现在的

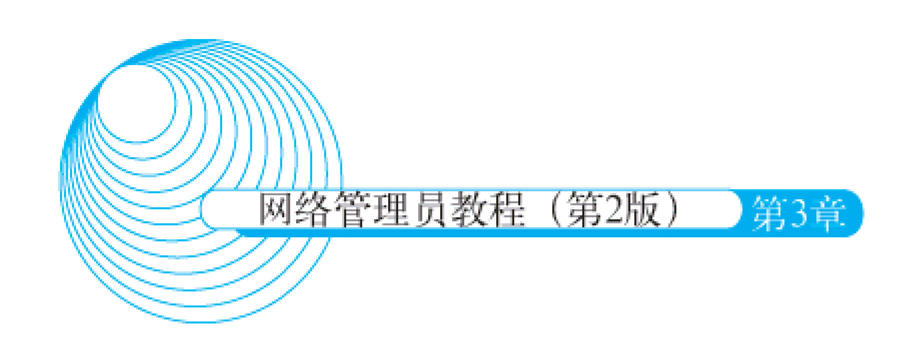
因特网的前身）。在访问 ARPANet 的过程中，他偶然发现了 ALOHA 系统（这是一个源于夏威夷大学的地面无线电广播系统，其核心思想是共享数据传输信道）的一篇论文，Metcalfe 认识到，通过优化就可以把 ALOHA 系统的速率提高到 100%。1972 年底，Metcalfe 和 David Boggs 设计了一套网络，把不同的 ALTO 计算机连接起来。Metcalfe 把他的这一研究性工作命名为 ALTO ALOHA。1973 年 5 月 22 日，世界上第一个个人计算机局域网 ALTO ALOHA 投入了运行，这一天，Metcalfe 写了一段备忘录，称他已将该网络改名为以太网，其灵感来自于“电磁辐射是可以通过发光的以太来传播的这一想法”。最初的以太网以 2.94Mbps 的速度运行，运行速度慢的原因是以太网的接口定时采用 ALTO 系统时钟，即每 340ns 才发送一个脉冲，构成了传输率为 2.94Mbps 的网络。当然，因为以太网的核心思想是使用共享的公共传输信道，在公共传输信道上进行载波监听，这已比初始的 ALOHA 网络有了巨大的改进，经过一段时间的研究与发展，1976 年，以太网已经发展到能够连接 100 个用户节点，并在 1000m 长的粗缆上运行。Xerox 急于将以太网转化为产品，因此将以太网改名为 Xerox Wire。1976 年 6 月，Metcalfe 和 David Boggs 发表了题为：“以太网：局域网的分布型信息包交换”的著名论文，1977 年底，Metcalfe 和他的 3 位合作者获得了“具有冲突检测的多点数据通信系统”的专利，多点传输系统被称为 CSMA/CD（载波监听多路访问/冲突检测）。从此，以太网就正式诞生了。

1979 年，在 DEC、Intel 和 Xerox 共同将此网络标准化时，同时将 Xerox Wire 网络又恢复成“以太网”这个原来的名字。1980 年 9 月，三方公布了第三稿的“以太网、一种局域网的数据链路层和物理层规范 1.0 版”，这就是著名的以太网蓝皮书，也称 DIX（DEC、Intel、Xerox 的第一个字母）版以太网 1.0 规范，一开始规范规定在 20MHz 下运行，经过一段时间后降为 10MHz，并重新定义了 DIX 标准，并以 1982 年公布的以太网 2.0 版规范终结。1983 年，以太网技术（IEEE 802.3）与令牌总线（IEEE 802.4）和令牌环（IEEE 802.5）共同成为局域网领域的 3 大标准。1995 年，IEEE 正式通过了 IEEE 802.3u 快速以太网标准，以太网技术实现了第一次飞跃，1998 年 IEEE 802.3z 千兆以太网标准正式发布，2002 年 7 月 18 日正式通过了万兆以太网标准 IEEE 802.3ae。

从 20 世纪 80 年代开始以太网就成为最普遍采用的网络技术，它一直“统治”着世界各地的局域网和企业骨干网，并且正在向城域网发起攻击。根据 IDC 的统计，以太网的端口数约为所有网络端口数的 85%，而且以太网的这种强大的优势仍然有继续保持下去的势头。纵观以太网的强劲发展历程，可以发现以太网主要得益于以下几个特点：

（1）开放标准，获得众多厂商的支持。目前，几乎所有的硬件制造商生产的设备，和几乎所有的软件开发商开发的操作系统和应用协议都与以太网兼容。

（2）易于移植和升级，可最大限度保护用户投资。对于所有以太网技术，其帧的结构几乎是一样的，这就提供了一个非常好的升级途径。快速以太网技术提供了从 10Mbps 向 100Mbps 以太网的平滑升级。千兆和万兆以太网的出现，增加带宽的同时也扩展了可升级性。只要将低速以太网设备用交换机连接到千兆和万兆以太网的设备上，就可实现一个物理线速向另一物理线



速的适配。这样的升级方式就使得千兆和万兆能无缝地与现在的以太网集成在一起。

（3）价格便宜，管理低成本。以太网技术无论在局域网、接入网还是即将进入的城域网、广域网在价格上与其他技术相比都具有优越性。若全面采用以太网解决方案，价格将更具有吸引力。另外，以太网存在时间长，标准化程度高，一般网络管理人员都比较熟悉，因此它的运行维护管理成本也比较低。

（4）结构简单，组网方便。以太网技术的实现原理统一采用了 CSMA/CD 媒体访问控制方法，不同版本的以太网的帧结构和网络拓扑结构也是一致的，对布线系统的要求较低，网络连接设备的配置比较简单。

3.2.2 以太网综述

1. 10Mbps 以太网

10Mbps 以太网根据传输介质的不同，大致有 4 个标准，各个标准的 MAC 子层媒体访问控制方法和帧结构，以及物理层的编码译码方法（曼彻斯特编码）均是相同的，不同的是传输媒体和物理层的收发器及媒体连接方式，依照技术出现的时间顺序，这 4 个标准依次是：

1）10Base5

1983 年 IEEE 802.3 工作组发布 10Base5“粗缆”以太网标准，这是最早的以太网标准。10Base5 以太网传输媒体采用 Φ10、50Ω 的粗同轴电缆，拓扑结构为总线型，电缆段上工作站之间的距离为 2.5m 的整数倍，每个电缆段内最多只能使用 100 台终端，但每个电缆段不能超过 500m。网络设计遵循“5—4—3”法则，根据该法则，整个网络的最大跨距为 2500m。

- “5”表示网络中任意两个端到端的节点之间最多只能有 5 个电缆段；
- “4”表示网络中任意两个端到端的节点之间最多只能有 4 个中继器；
- “3”表示网络中任意两个端到端的节点之间最多只能有 3 个共享网段。

10Base5 代表的具体意思是：工作速率为 10Mbps，采用基带信号，每一个网段最长为 500m。

2）10Base2

1986 年 IEEE 802.3 工作组发布 10Base2“细缆”以太网标准。10Base2 以太网传输媒体采用 ϕ5、50Ω 粗同轴电缆，拓扑结构为总线状，电缆段上工作站之间的距离为 0.5m 的整数倍，每个电缆段内最多只能使用 30 台终端，但每个电缆段不能超过 185m。10Base2 以太网设计遵循“5—4—3”法则，整个网络的最大跨距为 925m。

10Base2 代表的具体意思是：工作速率为 10Mbps，采用基带信号，每一个网段最长约为 200m。

3）10BaseT

1991 年 IEEE 802.3 工作组发布 10BaseT“非屏蔽双绞线”以太网标准。10BaseT 以太网传

输媒体采用 100Ω UTP 双绞线，拓扑结构为星型，即所有站点均连接到一个中心集线器上，但每个电缆段不能超过 100m。10BaseT 以太网设计遵循“5—4—3”法则，整个网络的最大跨距为 500m。

10BaseT 代表的具体意思是：工作速率为 10Mbps，采用基带信号，T 表示的是传输媒体双绞线（Twisted Pair）。

4）10BaseF

1993 年 IEEE 802.3 工作组发布 10BaseF“光纤”以太网标准。10BaseF 以太网传输媒体采用多模光纤，拓扑结构为星型，所有站点均连接到一个支持光纤接口的中心集线器上，每个电缆段不能超过 2000m。10BaseF 以太网设计也遵循“5—4—3”法则，但由于受 CSMA/CD 碰撞域的影响，整个网络的最大跨距为 4000m。

10BaseF 代表的具体意思是：工作速率为 10Mbps，采用基带信号，F 表示的是传输媒体光纤（Fiber）。

2. 百兆以太网

1995 年，IEEE 通过了 IEEE 802.3u 标准，将以太网的带宽扩大为 100Mbps。从技术角度上讲，IEEE 802.3u 并不是一种新的标准，只是对现存 IEEE 802.3 标准的升级，习惯上称为快速以太网。其基本思想很简单：保留所有的旧的分组格式，接口以及程序规则，只是将位时从 100ns 减少到 10ns，并且所有的快速以太网系统均使用集线器。快速以太网除了继续支持在共享介质上的半双工通信外，1997 年，IEEE 通过了 IEEE 802.3x 标准后，还支持在两个通道上进行的双工通信。双工通信进一步改善了以太网的传输性能。另外，100Mbps 以太网的网络设备的价格并不比 10Mbps 的设备贵多少。100BaseT 以太网在近几年的应用得到非常快速的发展。

1）100BaseT4

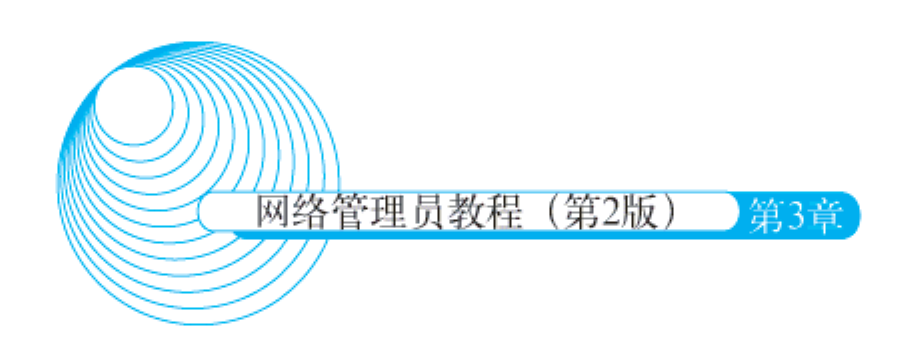
100BaseT4 传输载体使用 3 类 UTP，它采用的信号速度为 25MHz，需要 4 对双绞线，不使用曼彻斯特编码，而是三元信号，每个周期发送 4 比特，这样就获得了所要求的 100Mbps，还有一个 33.3Mbps 的保留信道。该方案即所谓的 8B6T（8 比特被映射为 6 个三进制位）。

2）100BaseTX

100BaseTX 传输载体使用 5 类 100Ω 的 UTP，其设计比较简单，因为它可以处理速率高达 125MHz 以上的时钟信号，每个站点只须使用两对双绞线，一对连向集线器，另一对从集线器引出。它采用了一种运行在 125MHz 下的被称为 4B/5B 的编码方案，该编码方案将每 4bit 的数据编成 5bit 的数据，挑选时每组数据中不允许出现多于 3 个 0，然后再将 4B/5B 码进一步编成 NRZI 码进行传输。这样获得 100Mbps 的数据传输速率，只需要 125MHz 的信号速率。

3）100BaseFX

100BaseFX 既可以选用多模光纤，也可以选用单模光纤，在全双工情况下，多模光纤传输距



离可达 2km，单模光纤传输距离可达 40km。

3. 千兆以太网

工作站之间用 100Mbps 以太网连接后，对于主干网络的传输速度就会提出更高的要求，1996 年 7 月，IEEE 802.3 工作组成立了 IEEE 802.3z 千兆以太网任务组，研究和制订千兆以太网的标准，这个标准满足以下要求：允许在 1000Mbps 速度下进行全双工和半双工通信；使用 IEEE 802.3 以太网的帧格式；使用 CSMA/CD 访问控制方法来处理冲突问题；编址方式和 10BaseT、100BaseT 兼容。这些要求表明千兆以太网和以前的以太网完全兼容。1997 年 3 月，又成立了另一个工作组 IEEE 802.3ab 来集中解决用 5 类线构造千兆以太网的标准问题，而 IEEE 802.3z 任务组则集中制订使用光纤和对称屏蔽铜缆的千兆以太网标准。IEEE 802.3z 标准于 1998 年 6 月由 IEEE 标准化委员会批准，IEEE 802.3ab 标准计划也于 1999 年通过批准。

1）1000BaseLX

1000BaseLX 是一种使用长波激光作为信号源的网络介质技术，在收发器上配置波长为 1270～1355nm（一般为 1300nm）的激光传输器，既可以驱动多模光纤，也可以驱动单模光纤。1000BaseLX 所使用的光纤规格如下：62.5μm 多模光纤，50μm 多模光纤，9μm 单模光纤。其中，使用多模光纤时，在全双工模式下，最长传输距离可以达到 550m；使用单模光纤时，全双工模式下的最长有效距离为 5km。系统采用 8B/10B 编码方案，连接光纤所使用的 SC 型光纤连接器与快速以太网 100BaseFX 所使用的连接器的型号相同。

2）1000BaseSX

1000BaseSX 是一种使用短波激光作为信号源的网络介质技术，收发器上所配置的波长为 770～860nm（一般为 800nm）的激光传输器不支持单模光纤，只能驱动多模光纤。具体包括以下两种：62.5μm 多模光纤，50μm 多模光纤。使用 62.5μm 多模光纤全双工模式下的最长传输距离为 275m；使用 50μm 多模光纤，全双工模式下最长有效距离为 550m。系统采用 8B/10B 编码方案，1000BaseSX 所使用的光纤连接器与 1000BaseLX 一样也是 SC 型连接器。

3）1000BaseCX

1000BaseCX 是使用铜缆作为网络介质的两种千兆以太网技术之一，另外一种就是将要在后面介绍的 1000BaseT。1000BaseCX 使用的一种特殊规格的高质量平衡双绞线对的屏蔽铜缆，最长有效距离为 25m，使用 9 芯 D 型连接器连接电缆，系统采用 8B/10B 编码方案。1000BaseCX 适用于交换机之间的短距离连接，尤其适合于千兆主干交换机和主服务器之间的短距离连接。以上连接往往可以在机房配线架上以跨线方式实现，不需要再使用长距离的铜缆或光纤。

4）1000BaseT

1000BaseT 是一种使用 5 类 UTP 作为网络传输介质的千兆以太网技术，最长有效距离与 100BaseTX 一样可以达到 100m。用户可以采用这种技术在原有的快速以太网系统中实现从

100Mbps 到 1000Mbps 的平滑升级。与在前面所介绍的其他 3 种网络介质不同，1000BaseT 不支持 8B/10B 编码方案，需要采用专门的更加先进的编码/译码机制。

4. 万兆以太网

1）10GE 以太网

2002 年 6 月，IEEE 802.3ae 10Gbps 以太网标准发布，以太网的发展势头又得到了一次增强。确定万兆以太网标准的目的是，将 IEEE 802.3 协议扩展到 10Gbps 的工作速度，并扩展以太网的应用空间，使之能够包括 WAN 链接。万兆以太网与 SONET OC-192 帧结构的融合，可以与 OC-192 电路和 SONET/SDH 设备一起运行，保护了传统基础设施投资，使供应商能够在不同地区中通过城域网提供端到端以太网。

（1）物理层：IEEE 802.3ae 大体分为两种类型，一种是与传统以太网连接，速率为 10Gbps 的 LAN PHY，另一种是连接 SDH/SONET，速率为 9.58464Gbps 的 WAN PHY。每种 PHY 分别可使用 10GBaseS（850nm 短波）、10GBaseL（1310nm 长波）、10GBaseE（1550nm 长波）3 种规格，最大传输距离分别为 300m、10km、40km，其中 LAN PHY 还包括一种可以使用 DWDM 波分复用技术的 10GBaseLX4 规格。WAN PHY 与 SONET OC-192 帧结构的融合，可与 OC-192 电路、SONET/SDH 设备一起运行，保护传统基础投资，使运营商能够在不同地区通过城域网提供端到端以太网。

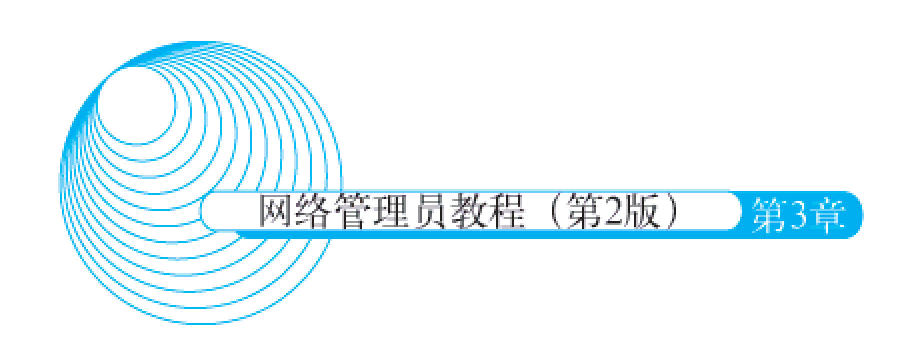
（2）传输介质层：IEEE 802.3ae 目前支持 9μm 单模、50μm 多模和 62.5μm 多模 3 种光纤，而对接口的支持规范 10GBaseCX4 目前正在讨论之中，尚未形成标准。

（3）数据链路层：IEEE 802.3ae 继承了 IEEE 802.3 以太网的帧格式和最大/最小帧长度，支持多层星型连接、点到点连接及其组合，充分兼容已有应用，不影响上层应用，进而降低了升级风险。与传统的以太网不同，IEEE 802.3ae 仅仅支持全双工方式，而不支持单工和半双工方式，不采用 CSMA/CD 机制。IEEE 802.3ae 不支持自协商，可简化故障定位，并提供广域网物理层接口。

人们不仅在万兆以太网的技术和性能方面看到了其实质性的提高，也正因如此，以太网正在从局域网逐步延伸至城域网和广域网，在更广阔的范围内发挥其作用。

2）40GE 以太网

2003 年 5 月 26 日，在以太网技术行将迎来 30 岁诞辰之际，思科高级副总裁 Luca Cafiero 指出，未来两年内，以太网最高数据传输速率将可望提高至 40Gbps。他称，业内将 40Gbps 而非 100Gbps 确定为以太网下一步发展目标的重要原因在于，与 100Gbps 以太网相比，研发 40Gbps 以太网在技术上面临的挑战相对较小，更为切实可行。与此同时，Cafiero 还指出，实际上，借助新发布的 Supervisor Engine 720 引擎，思科公司的 Catalyst6500 旗舰级企业交换平台目前已可以为每一接口卡提供 40Gbps 的数据传输速率支持。他还指出，新型以太网技术成功的关键在



于能够推动单位数据传输成本的下降。也就是说，新的以太网技术的 1bps 数据传输成本必须低于原有技术才能大获成功。

3.2.3 以太网技术基础

1. IEEE 802.3 帧的结构

媒体访问控制子层（MAC）的功能是以太网的核心技术，它决定了以太网的主要网络性能。MAC 子层通常又分成帧的封装/解封和媒体访问控制两个功能模块。在讨论该子层的功能时，首先要了解以太网的帧结构，其帧结构如图 3-7 所示。

7	1	6	6	2	46～1500	4
前导码	帧首定界符（SFD）	目的地址（DA）	源地址（SA）	长度（L）	逻辑链路层协议数据单元（LLC-PDU）	帧检验序列（FCS）

图 3-7 IEEE 802.3 帧的结构

（1）前导码：包含了 7 个字节的二进制“1”、“0”间隔的代码，即 1010…10 共 56 位。当帧在媒体上传输时，接收方就能建立起位同步，因为在使用曼彻斯特编码情况下，这种“1”、“0”间隔的传输波形为一周期性方波。

（2）帧首定界符（SFD）：它是长度为 1 个字节的 10101011 二进制序列，此码一过，表示一帧实际开始，以使接收器对实际帧的第一位定位。也就是说实际帧是由余下的 DA＋SA＋L＋LLCPDU＋FCS 组成。

（3）目的地址（DA）：它说明了帧企图发往目的站的地址，共 6 个字节。可以是单址（代表单个站）、多址（代表一组站）或全地址（代表局域网上所有的站）。当目的地址出现多址时，即表示该帧被一组站同时接收，称为“组播（Multicast）”。当目的地址出现全地址时，即表示该帧被局域网上所有站同时接收，称为“广播（Broadcast）”。通常以 DA 的最高位来判断地址的类型，若最高位为“0”则表示单址，为“1”表示多址或全地址，全地址时 DA 字段为全“1”代码。

（4）源地址（SA）：它说明发送该帧站的地址，与 DA 一样占 6 个字节。

（5）长度（L）：共占 2 个字节，表示 LLCPDU 的字节数。

（6）数据链路层协议数据单元（LLCPDU）：它的范围处在 46～1500 字节之间。

注意：最小 LLCPDU 长度 46 字节是一个限制，目的是要求局域网上所有的站都能检测到该帧，即保证网络正常工作。如果 LLCPDU 小于 46 个字节，则发送站的 MAC 子层会自动填充“0”代码补齐。

（7）帧检验序列（FCS）：它处在帧尾，共占 4 字节，是 32 位冗余检验码（CRC），检验除前导

码、SFD 和 FCS 以外的所有帧的内容，即从 DA 开始至 DATA 完毕的 CRC 检验结果都反映在 FCS 中。当发送站发出帧时，一边发送，一边逐位进行 CRC 检验。最后形成一个 32 位 CRC 检验和填在帧尾 FCS 位置中一起在媒体上传输。接收站接收后，从 DA 开始同样边接收边逐位进行 CRC 检验。最后接收站形成的检验和若与帧的检验和相同，则表示媒体上传输帧未被破坏。反之，接收站认为帧被破坏，则会通过一定的机制要求发送站重发该帧。

那么一个帧的长度为：

$$DA+SA+L+LLCPDU+FCS=6+6+2+(46\sim1500)+4=64\sim1518$$

即，当 LLCPDU 为 46 字节时，帧最小，帧长为 64 字节；当 LLCPDU 为 1500 字节时，帧最大，帧长为 1518 字节。

2. 以太网的跨距

系统的跨距表示了系统中任意两个站点间的最大距离范围，媒体访问控制方式 CSMA/CD 约束了整个共享型快速以太网系统的跨距。

前面介绍了 CSMA/CD 的重要的参数碰撞槽时间，可以认为：

$$\text{slot time}\approx 2S/0.7C+2t_{PHY}$$

如果考虑一段媒体上配置了中继器，且中继器的数量为 N，设一个中继器的延时为 tr，则：

$$\text{slot time}\approx 2S/0.7C+2t_{PHY}+2N\times tr$$

由于 slot time$=L_{min}/R$，L_{min} 称为最小帧长度，R 为传输速率，则系统跨距 S 的表达式为：

$$S\approx 0.35C\times(L_{min}/R\text{-}2t_{PHY}-2N\times tr)$$

通过前面的学习可知，$L_{min}=64B=512b$，$C=3\times10^8$ m/s，所以在 10Mbps 以太网环境中，$R=10\times10^6$ bps，在 100Mbps 以太网环境中，$R=100\times10^6$ bps。

如果忽略 $2t_{PHY}$ 和 $2N\times tr$，10Mbps 以太网环境中最大跨距为 5376m，100Mbps 以太网环境中最大跨距为 537.6m。在实际应用中如果忽略中继器，只算上 $2t_{PHY}$，10Mbps 以太网环境中最大跨距为 5000m 左右，100Mbps 以太网环境中最大跨距约为 412m。然而，在实际应用中，物理层所耗去的时间和中继器所耗去的时间都是不能忽略的，这也就是为什么要有 5－4－3 法则的原因。尤其是在 R 变大时跨距成几何级数递减，当 R 为 1000Mbps 时，依据这个法则，根据物理层所耗去的时间的大小，甚至会出现跨距为负的情况，则网络变得不可用。为此，在 1Gbps 以太网上采用了帧的扩展技术，目的是为了在半双工模式下扩展碰撞域，达到增长跨距的目的。

帧扩展技术是在不改变 IEEE 802.3 标准所规定的最小帧长度情况下提出的一种解决办法，把最小帧长一直扩展到 512 字节即 4096 位。若形成的帧小于 512 字节，则在发送时要在帧的后面添上扩展位，达到 512 字节发送到媒体上去。扩展位是一种非“0”、“1”数值的符号，若形成的帧已大于或等于 512 字节，则发送时不必添加扩展位。这种解决办法使得在媒体上传输的帧长度最短不会小于 512 字节，在半双工模式下大大扩展了碰撞域，媒体的跨距可延伸至

330m。在全双工模式下，由于不受 CSMA/CD 约束，无碰撞域概念，因此全双工模式下，在媒体上的帧无必要扩展到 512 字节。

100BaseTX/FX 系统的跨距如图 3-8 所示。由于跨距实际上反映了一个碰撞域，因此图中用两个 DTE 之间的距离来表示，DTE 可以是一个网桥、交换器或路由器，也可以认为是系统中两个站点。中继器(Repeater)用 R 表示一般是一个共享型集线器，它的功能是延伸媒体和连接另一个媒体段。

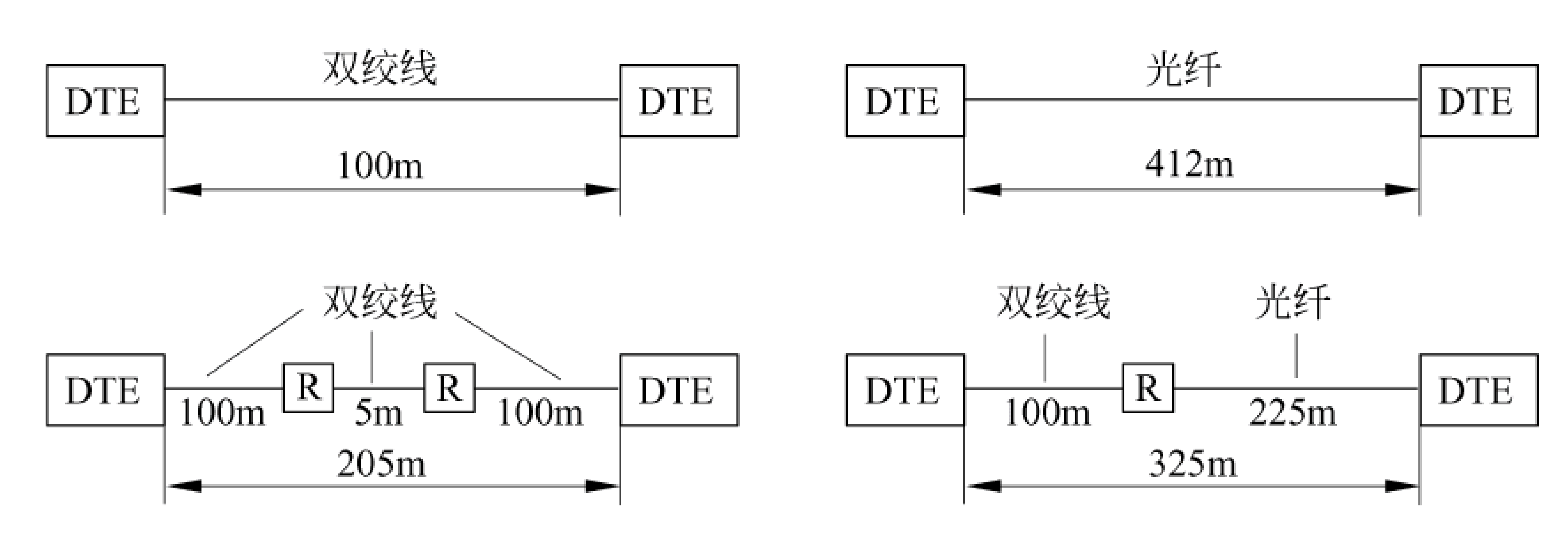


图 3-8　100Mbps 以太网的跨距

在双绞线媒体情况下，由于最长媒体段距离为 100m，加 1 个中继器，就延伸 1 个最长媒体段距离，达到 200m。如果再想延伸距离时，加 2 个中继器后，也只能达到 205m，205m 即为 100BaseTX 的跨距。

在光纤媒体情况下，不使用中继器，跨距可达到 412m，即是 1 个碰撞域范围，但光纤的最长媒体段 2km 要远远大于 412m。另外，加 1 个中继器后，并不能延伸距离，由于中继器的延迟时间，跨距反而变小了，在加 2 个中继器时，跨距几乎和双绞线加 2 个中继器的跨距相同。因此，在实际应用中通常采用混合方式，即中继器一侧采用光纤，另一侧采用双绞线。双绞线可直接连接用户终端，跨距可达 100m，光纤可直接连接路由器或主干全双工以太网交换机，跨距可达 225m。

3. 交换型以太网

在交换型以太网出现以前，以太网系统均为共享型以太网系统。在整个系统中，受到 CSMA/CD 媒体访问控制方式的制约。整个系统处在一个碰撞域范围中，系统中每个站都可能在往媒体上发送帧，那么每个站要占用媒体的机率就是 10Mbps/n，n 为站数。以太网受到 CSMA/CD 制约后，所有的站均在争用媒体而共同分割带宽，称“共享型”以太网。

在 20 世纪 80 年代后期，即 10BaseT 出现后不久，就出现了以太网交换型集线器。到了 20 世纪 90 年代，快速以太网的交换技术和产品更是发展迅速，广泛应用。交换型以太网系统中的交换型集线器，也称以太网交换器，以其为核心连接站点或者网段。如图 3-9 所示，交换器的各端口之间在交换器上同时可以形成多个数据通道，图中在交换器上同时存在了 4 个数据通道，

它们可以存在于站与站，站与网段或者网段与网段之间。网段即是多个站点构成一个共享媒体的集合，一般是一个共享型集线器连接若干个站点构成一个网段。

既然是在交换器上同时存在多个端口间的通道，也就意味着系统同时存在多个碰撞域，每一个碰撞域的一对端口都独占带宽（一个享有发送带宽，另一个享有接收带宽），那么就整个系统的带宽来说，就不再是只有 10Mbps（10BaseT 环境）或 100Mbps（100BaseT 环境），而是与交换器所具有的端口数有关。可以认为，若每个端口为 10Mbps，则整个系统带宽可达 10Mbps $\times n$，其中 n 为端口数，若 $n=10$，则系统带宽可达 100Mbps。因此，拓宽整个系统带宽是交换型以太网系统的最明显的特点。

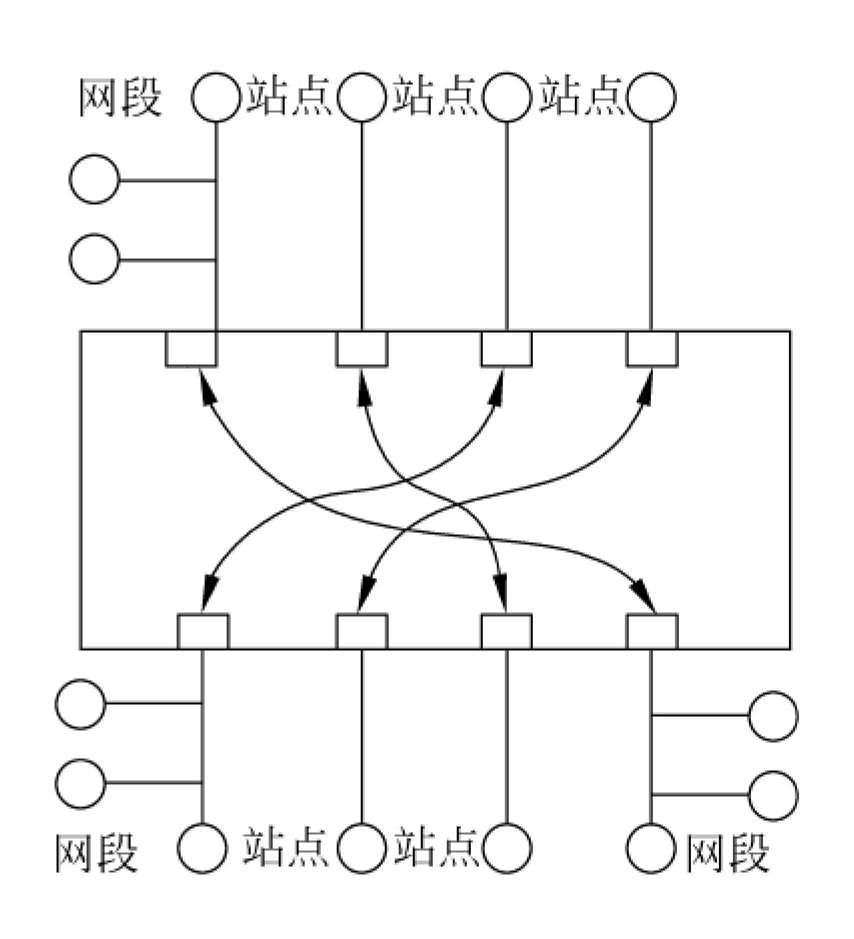


图 3-9　以太网交换器示意

综上所述，交换型以太网系统与共享型以太网比较有如下优点：

（1）每个端口上可以连接站点，也可以连接一个网段。不论站点和网段均独占该端口的带宽（10Mbps 或 100Mbps）。

（2）系统的最大带宽可以达到端口带宽的 n 倍，其中 n 为端口数。n 越大，系统的带宽越高。

（3）交换器连接了多个网段，每一个网段都是独立的，被隔离的。但如果需要的话，独立网段之间通过其端口也可以建立暂时的数据通道。

（4）被交换器隔离的独立网段上数据流信息不会随意广播到其他端口上去，因此具有一定的数据安全性。

4．全双工以太网

交换器设备工作时不同的逻辑数据通道之间已不再受到 CSMA/CD 的约束，但每条逻辑数据通道的两个端口之间，却仍然受到 CSMA/CD 的约束。即一条逻辑数据通道就是一个碰撞域。

当交换器以太网技术和应用发展到一定阶段后，不仅要求整个系统的带宽要达到一定高度，而且还要求整个系统的跨距也要有一定的保证，特别在 100Mbps 及 1Gbps 以太网环境中，使用光纤作为媒体的情况下，若再使用受到 CSMA/CD 约束的一般半双工技术和产品的话，则网络覆盖范围的矛盾尤为突出。为了解决上述的问题，全双工以太网技术和产品问世了，且在 1997 年由 IEEE 802.3x 标准来说明该技术的规范。

全双工以太网技术是用来说明以太网设备端口的传输技术，与传统半双工以太网技术区别

在于：每个端口和交换机背板之间都存在两条逻辑通路。这样，每一个端口就可以同时接收和发送帧，不再受到CSMA/CD的约束，在端口发送帧时不再会发生帧的碰撞，已无碰撞域的存在。这样一来，端口之间媒体的长度仅仅受到数字信号在媒体上传输衰变的影响，而不像传统以太网半双工传输时还要受到碰撞域的约束。

图3-10所示为两个端口之间全双工传输的特点。端口上设有端口控制功能模块和收发器功能模块，端口上的全双工还是半双工操作一般可以自适应，也可以用人工设置。当全双工操作时，帧的发送和接收可以同时进行，这样与传统半双工操作方式比较，传输链路的带宽提高了一倍，即端口支持10Mbps或者100Mbps传输率，而其带宽却分别是20Mbps和200Mbps。在全双工传输帧时，端口上既无侦听的机制，链路上又不会多路访问，也不再需要碰撞检测，传统半双工方式下的媒体访问控制CSMA/CD的约束已不存在。

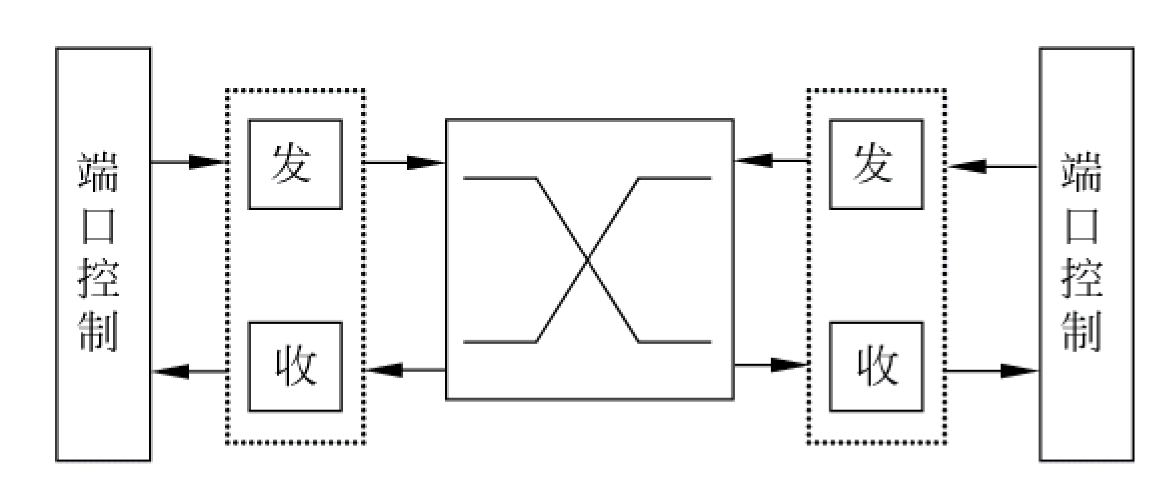


图3-10　全双工以太网交换器示意

在10Mbps端口传输率情况下，只有10BaseT及10BaseFL支持全双工操作，而在100Mbps快速以太网情况下，除了100BaseT4外，100BaseFX和100BaseTX均支持全双工操作，1000BaseX也支持全双工操作。即只有链路上提供独立的发送和接收媒体才能支持全双工操作。表3-1说明了支持全双工操作的各类以太网网段的最长距离，并与传统半双工操作受碰撞域限定的网段最长距离进行比较。

从表3-1可知，使用双绞线媒体，100m的距离对于半双工操作来说并非是碰撞域的跨距，仍是数字信号驱动的最长距离，因此不论是10Mbps、100Mbps环境，还是1000Mbps环境，全双工操作并未占有优势。对于媒体采用光纤来说，10BaseFL在两种情况下，光纤最长距离均为2km，这是因为在10Mbps传输速率情况下，由碰撞域决定的半双工网段最长距离要大于2km，2km的光纤仍是由数字信号在光纤上传输的最长距离。在100BaseFX的以太网中，全双工网段距离可达2km，而传统的半双工操作情况下，由于受到CSMA/CD的约束，碰撞域的跨距决定了网段最长距离为412m。在1000BaseLX的以太网中，采用单模光纤全双工网段距离可达5km，而传统的半双工操作情况下，由于受到CSMA/CD的约束，碰撞域的跨距决定了网段最长距离为330m。在1000BaseSX的以太网中，因不能使用单模光纤，多模光纤扩展网络有效距离的效果并不明显。

表 3-1 以太网网段的最长距离

以太网类型	传输媒体	全双工网段最长距离	半双工网段最长距离
10BaseT	UTP	100m	100m
10BaseF	MMF	2km	2km
100BaseT	UTP、STP	100m	100m
100BaseF	MMF	2km	412m
1000BaseLX	MMF	550m	330m
	SMF	5km	330m
1000BaseSX	MMF62.5μm	300m	
	MMF50μm	550m	330m
1000BaseCX	STP	25m	25m
1000BaseT	UTP	100m	100m

对于网络中的客户机而言，由于其访问服务器时，发送和接收的负载往往是很不均衡的，因此，用全双工操作方式连接客户站，可延伸距离有明显的收益。对于服务器，由于会受到许多客户站的同时访问，所以发送和接收的负载一般较接近均衡，所以使用全双工操作方式，可增加带宽是明显的收益，但由于系统服务器往往与系统主交换器放置在一起，因此在延伸距离上显得无必要。对于交换器之间的连接来说，使用全双工操作方式，在延伸连接距离和拓展带宽上均能收益。

3.2.4 以太网交换机的部署

在应用级的局域网中，很少存在只使用单台交换机的局域网。一方面，因为单台交换机的端口数量有限，另一方面，单台交换机的地理位置使得联网计算机终端的距离受限。通常，在一个局域网中，使用几台交换机互相连接在一起，从而达到扩展端口和扩展距离的目的。那么交换机与交换机是如何连接在一起的呢？目前广泛使用的模式有两种，一种是级连（Uplink）模式，另一种是堆叠（Stack）模式。

1. 级连模式

级连模式是最常规，最直接的一种扩展方式。级连模式是通过双绞线或光纤，一般在交换机的前面板上有专门的级连口，如果没有，也可以用交叉接法来级连。级连是通过端口进行的，级连后两台交换机是上下级的关系。

级连模式起源于早期的共享型集线器，共享型集线器的物理拓扑结构是星型，而逻辑拓扑

结构还是总线型的，集线器仅仅相当于一条浓缩了的总线，在集线器的某一个端口，级连另一台集线器，只是相当于把浓缩的总线又加长了一些，仍然是一条总线，所有端口都要在一个碰撞域里受到 CSMA/CD 的约束。但这样相当于把传输媒体加长了，在加长的传输媒体上又增加了一些端口。但付出的代价是，在这个碰撞域里，又多了一些端口共享整个带宽，从而导致网络性能低下。当然这种级连方式，必须遵循 5—4—3 法则，也就是级连不能超过 4 层。级连模式的典型结构如图 3-11 所示。

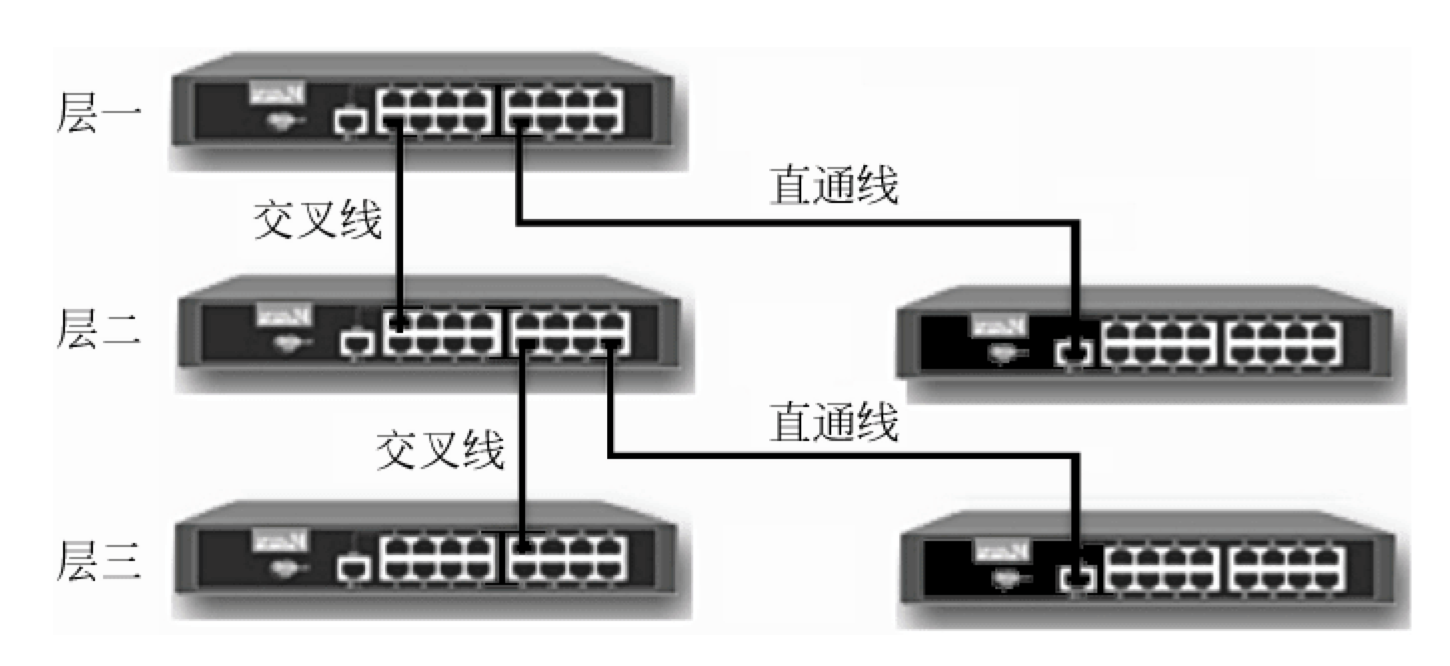


图 3-11 级连模式的以太网交换机

需要特别指出的是，对于那些没有专用级连端口的集线器之间的级连，双绞线接头中线对的分布与连接网卡和集线器时有所不同，必须要用交叉线。而许多集线器为了方便用户，提供了一个专门用来串接到另一台集线器的端口，在对此类集线器进行级连时，双绞线均应为直通线接法。不管采用交叉线还是直通线进行级连，都没有改变级连的本质。

用户如何判断集线器是否需要交叉线连接呢？主要方法有以下几种：

(1) 查看说明书。如果该集线器在级连时需要交叉线连接，一般会在设备说明书中进行说明。

(2) 查看连接端口。如果该集线器在级连时不需要交叉线，大多数情况下都会提供一至两个专用的互连端口，并有相应标注，如 Uplink、MDI、Out to Hub，表示使用直通线连接。

(3) 实测。这是最管用的一种方法。可以先制作两条用于测试的双绞线，其中一条是直通线，另一条是交叉线。之后，用其中的一条连接两个集线器，这时观察连接端口对应的指示灯，如果指示灯亮表示连接正常，否则换另一条双绞线进行测试。

随着快速以太网技术和交换技术的出现，级连模式又逐渐变成组建大型局域网最理想的扩展方式，成为以太网扩展端口应用中的主流技术。在交换机上进行级连，级连交换机的端口共享的仅仅是被级连交换机中被级连端口的带宽，而不是整个网络的带宽。更何况目前的交换机级连通常都是高速交换机端口级连低速交换机，即 1000Mbps 端口，级连 100Mbps 的交换机；100Mbps 端口，则级连 10Mbps 的交换机；或者是交换机级连共享型的集线器。由此一来，极大程度地克服了传统集线器级连共享带宽，而导致网络性能降低的弊端。虽然交换机的级连在一

定程度上仍然受 CSMA/CD 的约束，但其优势却是不可替代的，通常表现在以下几个方面：

(1) 级连模式可使用通用的以太网端口进行层次间互联，其中包括 100Mbps 端口、1000Mbps 端口以及新兴的 10Gbps 端口。

(2) 级连模式是组建结构化网络的必然选择，级连使用普通的、长度限制并不严格的电缆(光纤)，各个级连单元的位置相对较随意，非常有利于综合布线。

(3) 级连模式通常是解决不同品牌的交换机之间以及交换机与集线器之间连接的有效手段。

2. 堆叠模式

堆叠通常是为了扩充带宽用的，通常用专门的堆叠卡插在交换机的后面，用专门的堆叠电缆连接几台交换机，堆叠后这几台交换机相当于一台交换机。堆叠是采用交换机背板的叠加，使多个工作组交换机形成一个工作组堆，从而提供高密度的交换机端口，堆叠中的交换机就像一个交换机一样，配制一个 IP 地址即可。

级连是通过交换机的某个端口与其他交换机相连的，而堆叠是通过交换机的背板连接起来的，它是一种建立在芯片级上的连接，如两个 24 口交换机堆叠起来的效果就像是一个 48 口的交换机。

堆叠模式的优点是：

(1) 增加网络端口的同时，还增加了逻辑数据通道，扩充了网络带宽，不同堆叠单元的端口之间可以直接交换，进行快速转发，从而极大地提高了网络性能。

(2) 不受 5—4—3 法则的约束，堆叠单元可以超过 4 个。

(3) 提供简化的本地管理，将一组交换机作为一个对象来管理。

堆叠模式的缺点是：

(1) 堆叠是一种非标准化技术，各个厂商之间不支持混合堆叠，同一组堆叠交换机必须是同一品牌。

(2) 堆叠模式不支持即插即用，在物理连接完毕之后，还要对交换机进行相应的设置，才能正常运行。

(3) 不存在拓扑管理，一般不能进行分布式布置。

常见的堆叠有两种：菊花链堆叠和矩阵堆叠。

(1) 菊花链就是从上到下串起来，形成单一的一个菊花链堆叠总线。菊花链模式是简化的级联模式，主要的优点是提供集中管理的扩展端口，对于多交换机之间的转发效率并没有提升，主要是因为菊花链模式是采用高速端口和软件来实现的。菊花链模式使用堆叠电缆将几台交换机以环路的方式组建成一个堆叠组，然后加一根从上到下起冗余备份作用的堆叠电缆。如图 3-12 所示的是 2003 年 6 月，北电网络推出的 BayStack 5510 菊花链堆叠交换机，一个堆叠中有 8

个交换机，整个堆叠的带宽高达640Gbps，每个交换机与上下相邻单元间都具有40Gbps的全双工带宽。

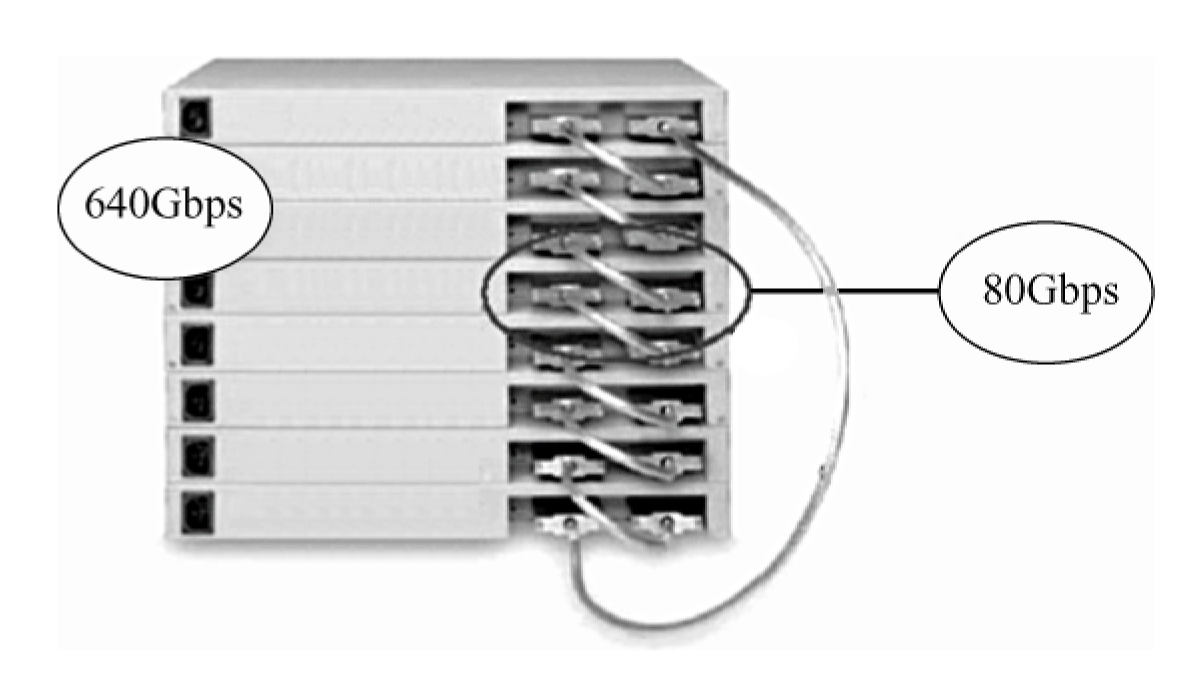


图3-12　菊花链堆叠交换机

（2）矩阵堆叠需要提供一个独立的或者集成的高速交换中心（堆叠中心），所有堆叠的交换机通过专用的高速堆叠端口上行到统一的堆叠中心，堆叠中心一般是一个基于专用ASIC的硬件交换单元，ASIC交换容量限制了堆叠的层数。使用高可靠、高性能的Matrix芯片是矩阵堆叠的关键。由于涉及到专用总线技术，电缆长度一般不能超过2m，所以，矩阵堆叠模式下，所有的交换机需要局限在一个机架之内。如图3-13所示的是3COM公司的3300系统交换机连成矩阵堆叠的示意图。

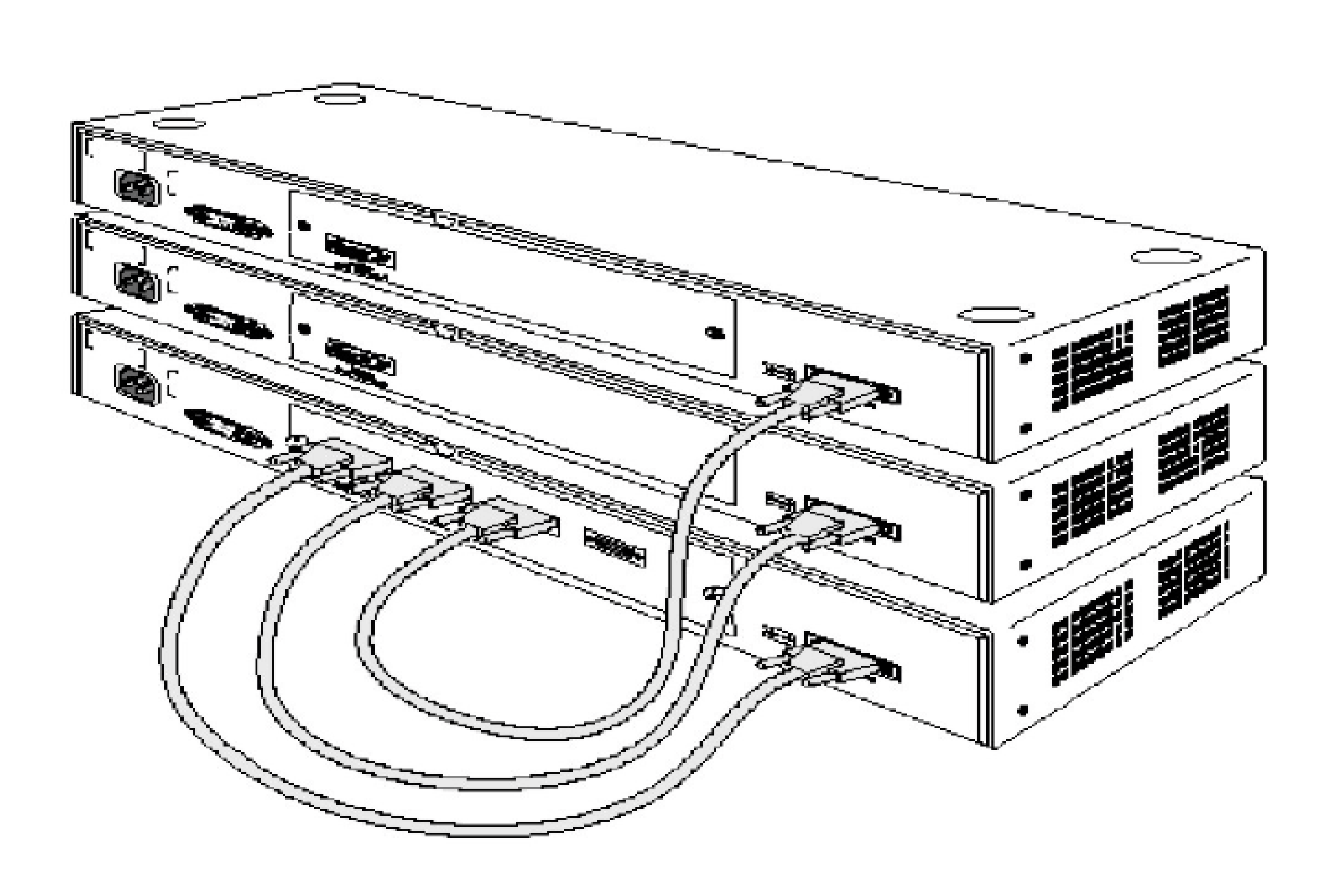


图3-13　矩阵堆叠交换机

3. 混合模式

通过前面的介绍，不难得出结论：堆叠模式是一种集中管理的端口扩展技术，不能提供拓扑

管理，没有国际标准，且兼容性较差。但是，对于那些对带宽要求较高并需要大量端口的单节点局域网，堆叠模式可以提供比较优秀的转发性能和方便的管理特性。级连模式是组建网络的基础，可以灵活利用各种拓扑、冗余技术，对于那些对带宽要求不高且级连层次很少的网络，级连方式可以提供最优化的性能。可见，级连模式和堆叠模式的优点和缺点都十分鲜明，单纯地运用任何一种模式，都不会最大限度地优化网络。在实际的应用中，由于网络的复杂性，用户需求的多重性，通常同时使用两种模式进行交换机的部署，称其为混合模式。图 3-14 所示的就是在考虑了半双工以太网最大跨距约束的一个典型的混合模式交换机部署方案。

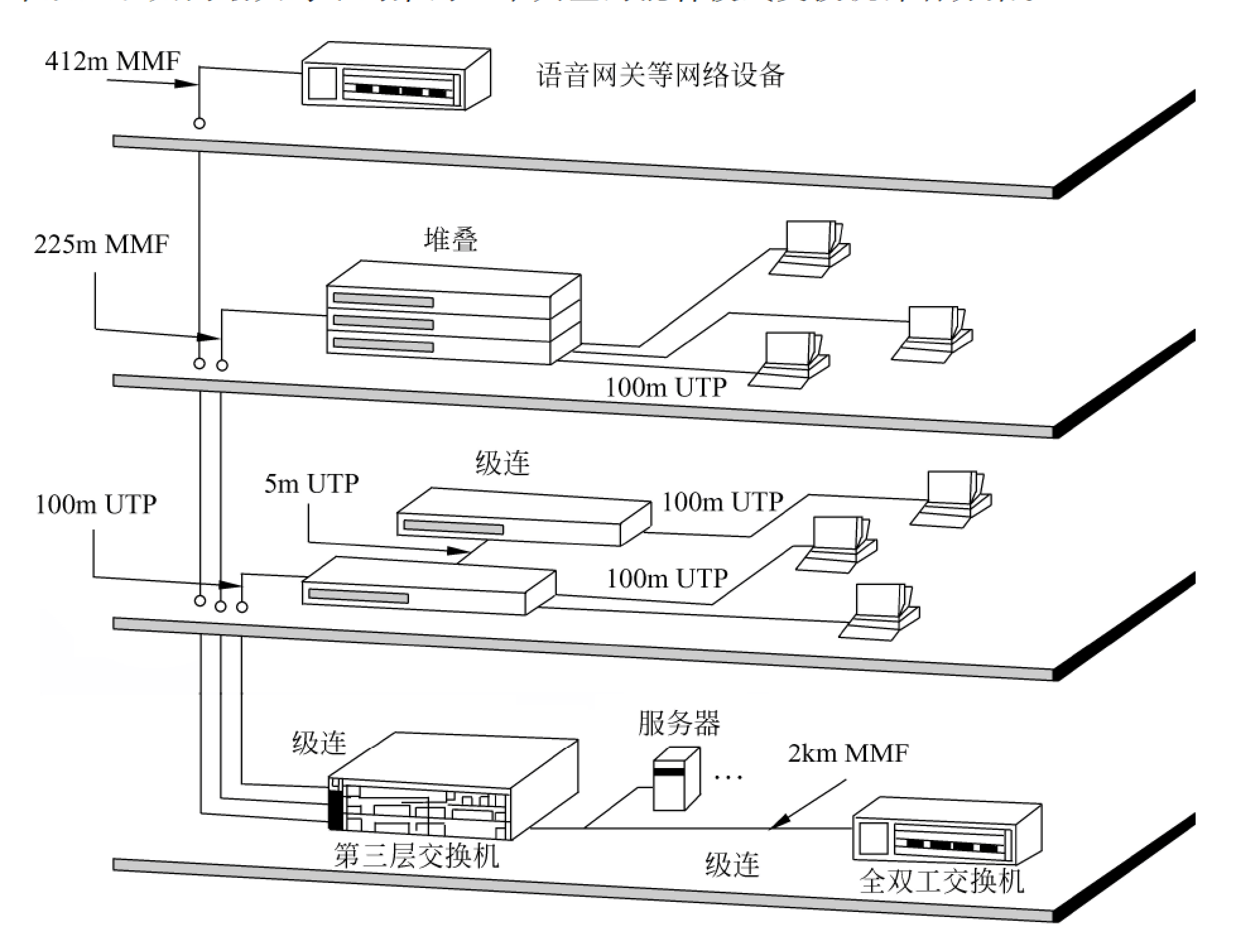
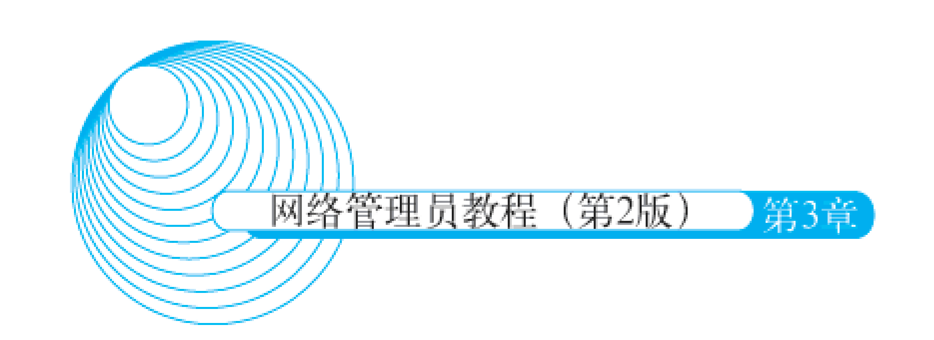


图 3-14　混合模式部署交换机

3.2.5　以太网交换机的设置

通常情况下，一台新的交换机部署到网络中后，使用它的默认配置就可以直接工作了，不需要再进行设置。因为它是一种将软件装在 FlashMemory 中的硬件设备，当加电时，它首先要进行一系列自检，对所有端口进行测试之后，交换机就处于工作状态。这时它的交换表是空的，它可以通过自学习来了解各个端口的设备连接情况，并将设备的 MAC 地址记录在交换表中，当有信息交换时，交换机就根据交换表来进行数据转发。但是，当有一些高级的应用和需求时，例



如，通过交换机划分 VLAN，对交换机进行远程管理，对关键设备的端口镜像进行入侵检测等。这些就需要对交换机进行设置。

通常对一台新的交换机进行配置和管理有两个大的步骤，一是通过仿真终端进行 IP 地址设置，二是通过浏览器进行管理。

大部分交换机本身都有一个 MAC 地址，可以通过仿真终端软件将这个 MAC 地址绑定一个 IP 地址，当然，这个 IP 地址应该是管理终端能够访问的。交换机有了 IP 地址后，就可以通过网络对它进行管理了。早期的交换机都使用 Telnet 命令行的方式对其进行远程管理。近期的交换机都提供了界面更为友好的 Web 管理方式，不同厂家交换机产品的设置方法大同小异。下面以 3COM 公司的 3300 系列交换机为例讲解交换机的设置方法。

1. 通过仿真终端进行 IP 地址设置

(1) 用一条 RS—232 电缆将管理终端的串口与交换机的控制台端口(Console)相连。交换机的 Console 通常在背面板上，如图 3-15 所示。

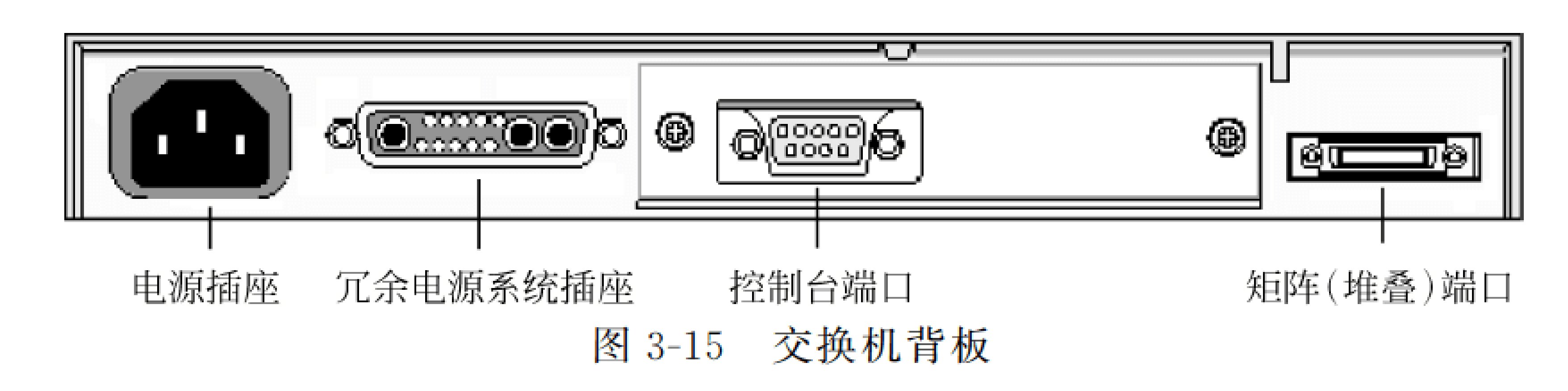


图 3-15 交换机背板

(2) 运行仿真终端软件，通常使用“附件”中的“超级终端”即可。打开“超级终端”，建立一个新的连接，如图 3-16 所示。



图 3-16 超级终端建立连接

（3）建立新连接时，在“连接时使用：”处选择连接时使用的设备或端口，此处选择 COM1，然后单击“确定”按钮，如图 3-17 所示。

（4）在 COM1 端口属性对话框中配置仿真终端的比特率、数据位、奇偶校验和停止位等参数，可参阅设备说明书提供的参数，通常也可利用自动检测的默认值。如图 3-18 所示，参数设置好后，单击“确定”按钮。



图 3-17 选择连接时使用的设备



图 3-18 配置 COM1 参数

（5）在“超级终端”窗口中出现交换机的登录界面，在“Login：”位置输入登录用户名，在“Password：”位置输入相应的口令。交换机通常提供了一些常见用户名，如 monitor、manager、security、admin、system 等，口令一般与用户名相同或者无。输入口令正确后，会出现交换机的字符菜单界面，每一个菜单后面都有简单的功能解释。在“Select menu option：”位置，输入 ip，选择 ip 菜单项，如图 3-19 所示。

（6）在“超级终端”窗口中出现 ip 菜单的子菜单项，如图 3-20 所示。在“Select menu option：”位置，输入 interface，选择接口子菜单项。

（7）在“超级终端”窗口中出现接口子菜单项的下一级菜单，如图 3-21 所示。在“Select menu option：”位置，输入 define，选择接口定义子菜单项。

（8）在“超级终端”窗口中出现接口定义的相应内容。在“Enter IP address：”位置，输入交换机的 IP 地址，在“Enter subnet mask：”位置，输入相应的子网掩码，即完成了交换机 IP 地址的设置，如图 3-22 所示。

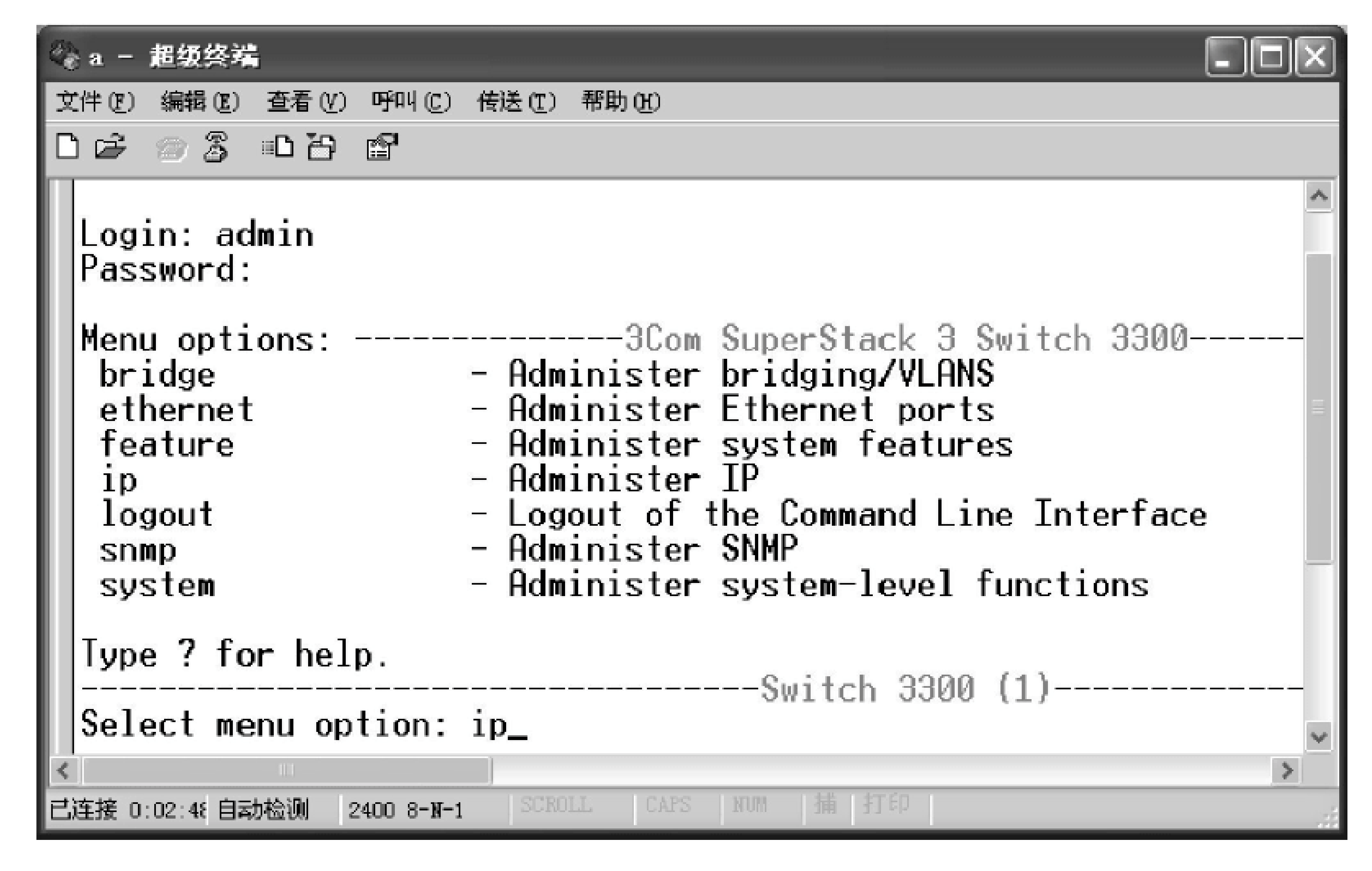


图 3-19　交换机 Console 配置的字符菜单界面输入 ip

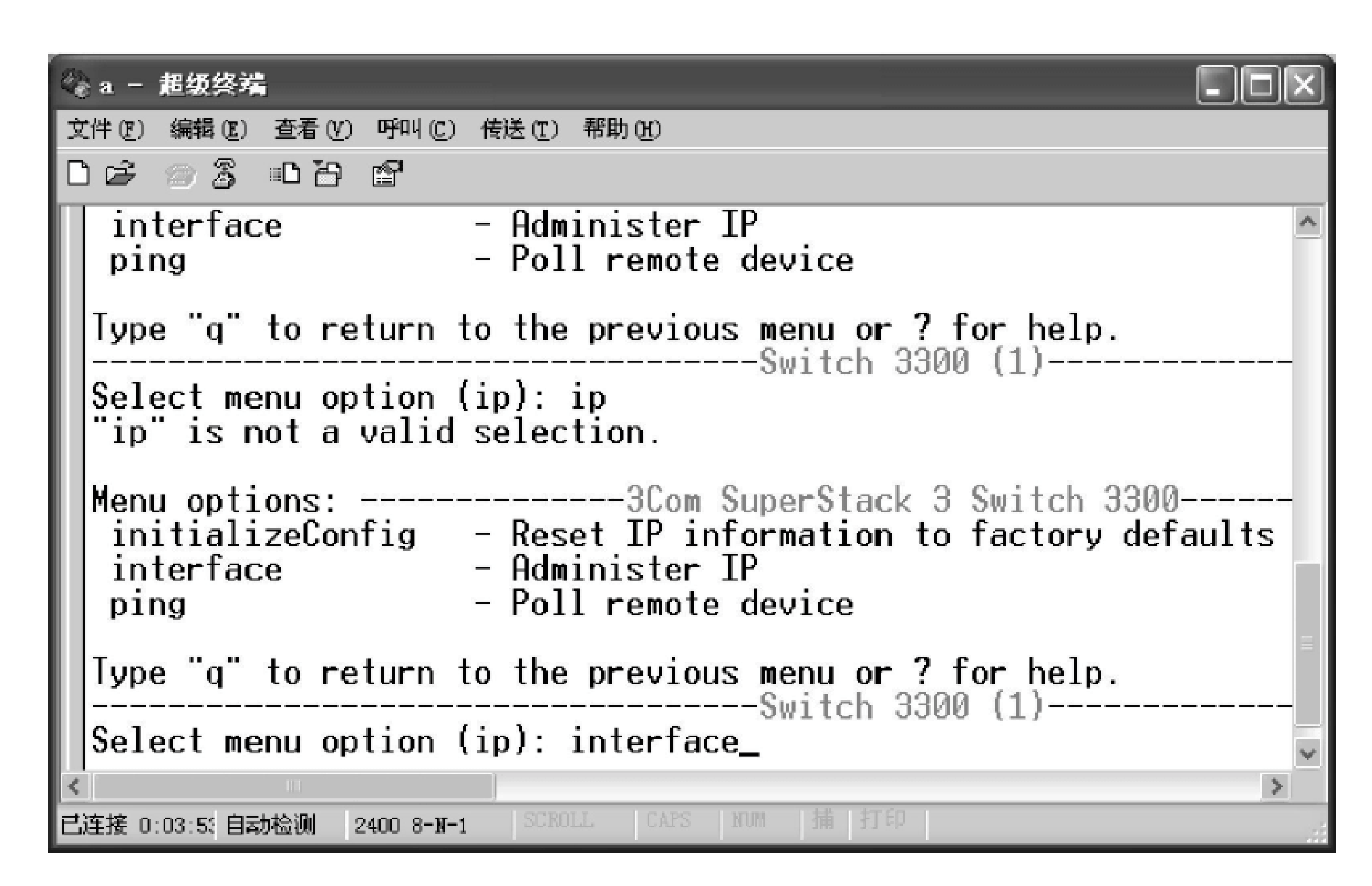


图 3-20　交换机 Console 配置的字符菜单界面输入 interface

2. 通过浏览器进行管理

(1) 打开浏览器，在 URL 栏中输入交换机的 IP 地址后按 Enter 键，会出现交换机的 Web 登录界面，如图 3-23 所示。在 Web 登录界面中输入相应的用户名和密码后，单击“确定”按钮。

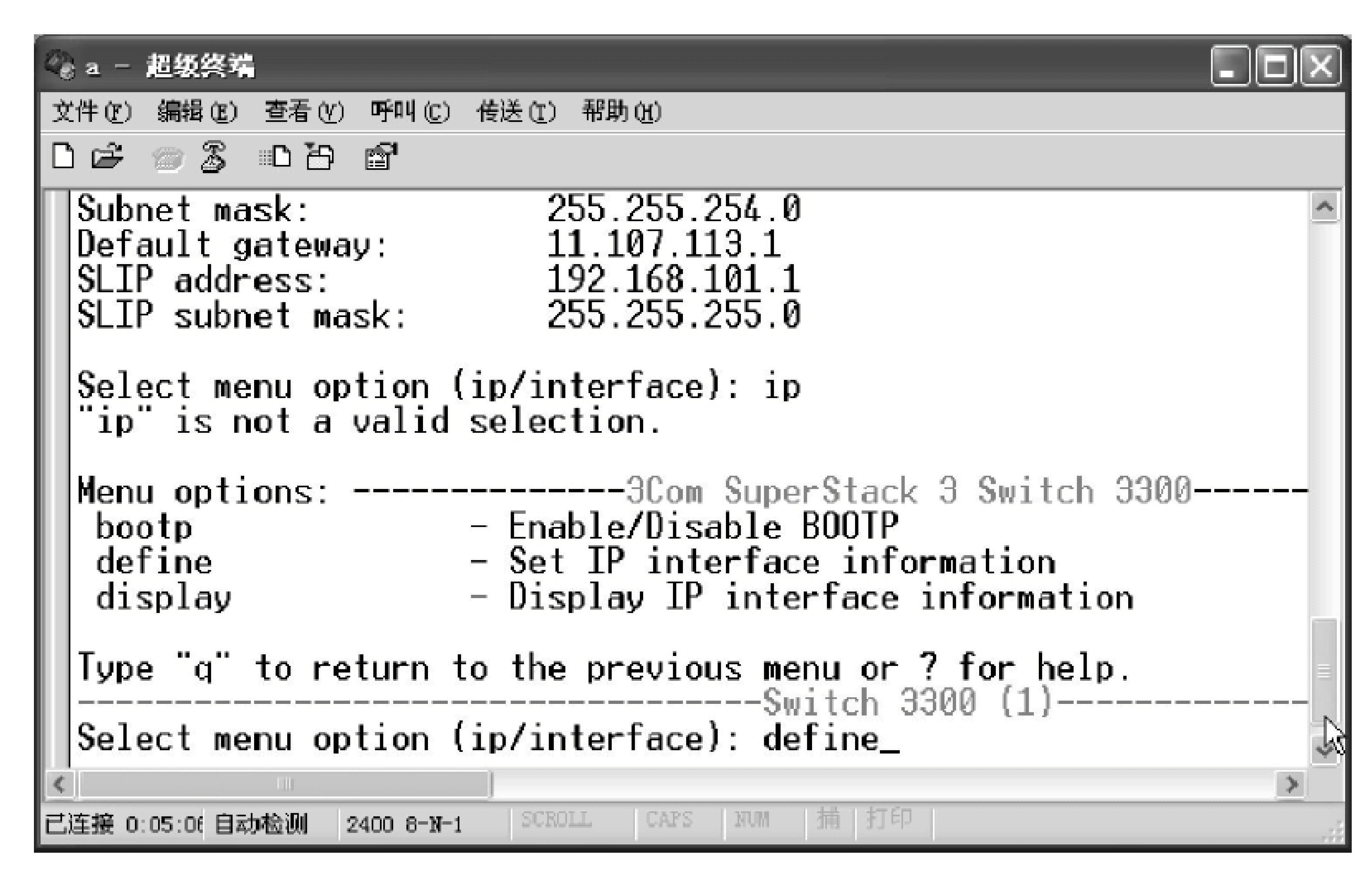


图 3-21　交换机 Console 配置的字符菜单界面输入 define

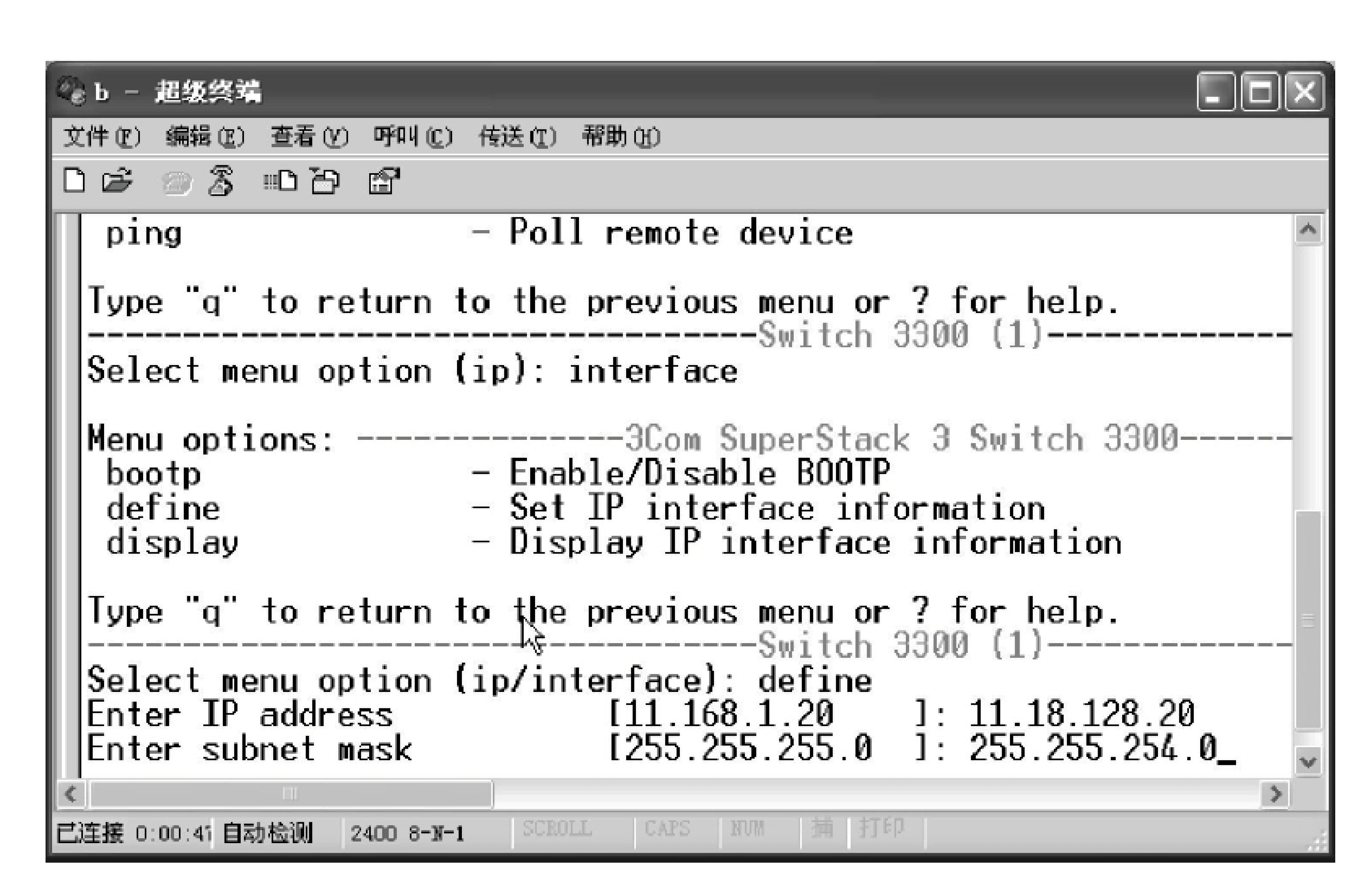


图 3-22　交换机 Console 配置的字符菜单界面输入 IP 地址及子网掩码

（2）在“浏览器”窗口中会出现交换机的 Web 管理页面，如图 3-24 所示。

（3）在 Web 管理页面中，既可以查看交换机的基本信息，也可以进行一些参数设置。如图 3-25 所示的就是查看交换机每一个端口的状态，图 3-26 所示的就是修改交换机管理用户的口令。

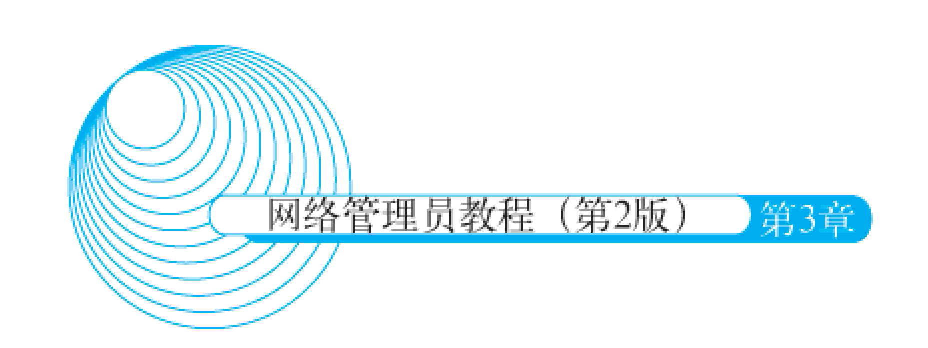




图 3-23 交换机 Web 管理的登录界面

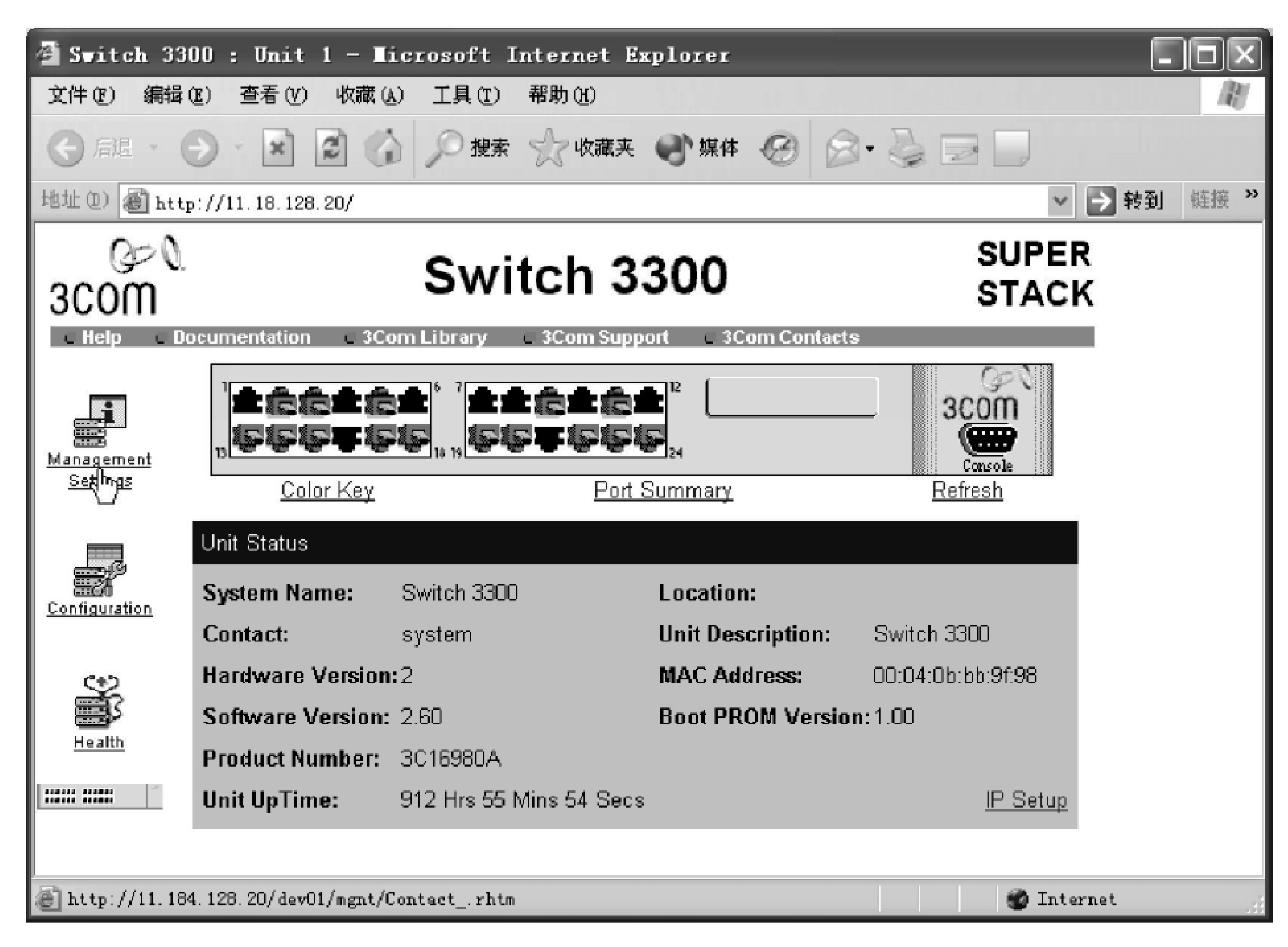


图 3-24 交换机 Web 管理页面

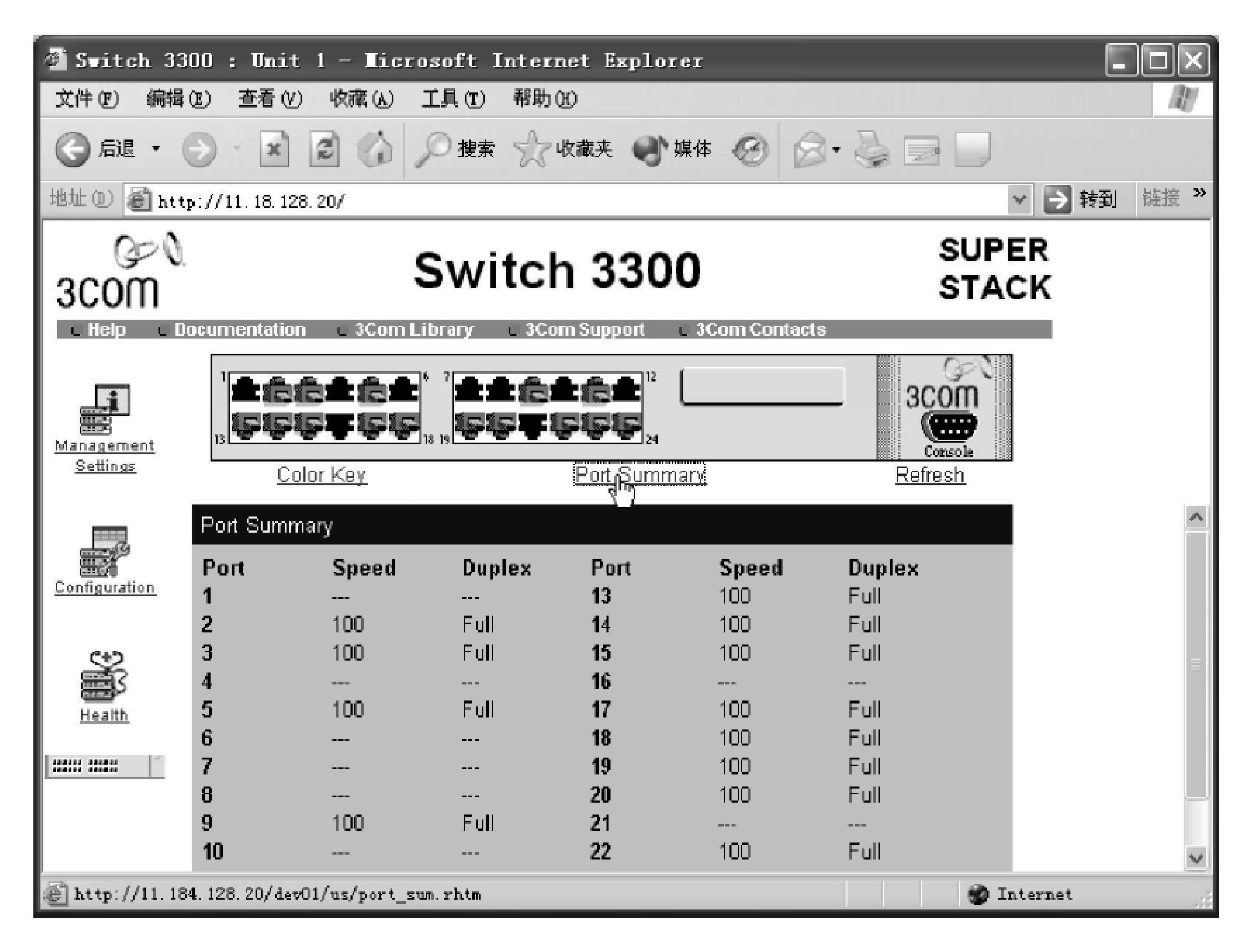


图 3-25　查看交换机端口状态

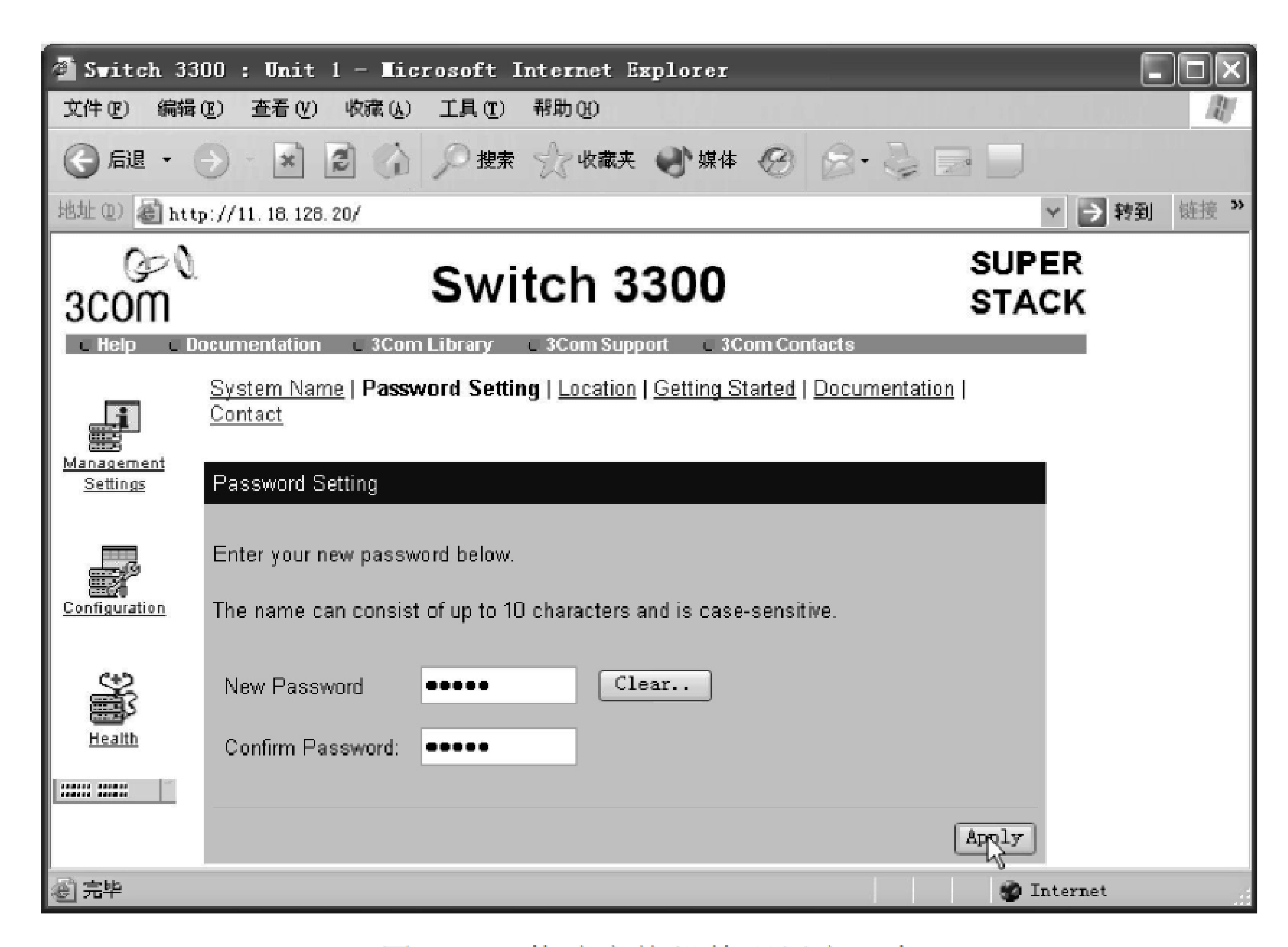
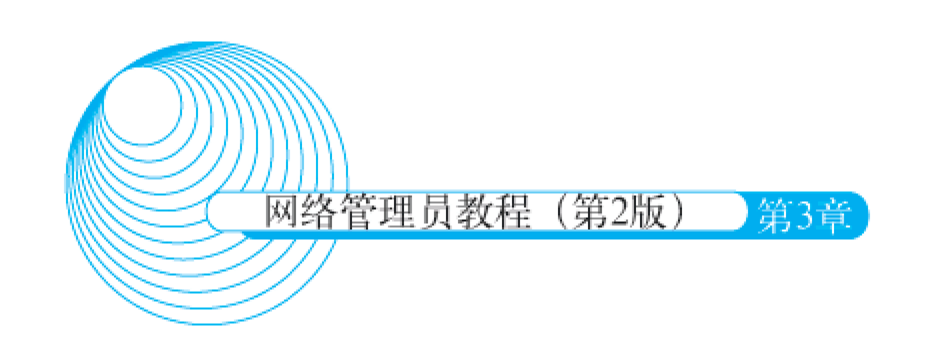


图 3-26　修改交换机管理用户口令



3.2.6 在以太网中划分 VLAN

1. VLAN 的概念

最早的 VLAN 技术早在 1996 年由 Cisco 公司提出。IEEE 于 1999 年 6 月颁布了用以标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准草案。随着几年来的发展，VLAN 技术得到广泛的支持，成为当前最为热门的一种以太局域网技术。

VLAN（Virtual Local Area Network）的中文名为“虚拟局域网”，是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

VLAN 技术的出现，使得管理员可以根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，并与物理上形成的 LAN 有着相同的属性。VLAN 示意图如图 3-27 所示。由于它是从逻辑上划分，而不是从物理上划分，所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理 LAN 网段上。这种基于工作流的分组模式，大大提高了网络规划和重组的管理功能。在同一个 VLAN 中的工作站，不论它们实际上与哪个交换机连接，它们之间的通信就好像在独立的交换机上一样。同一个 VLAN 中的广播只有 VLAN 中的成员才能听到，而不会传输到其他的 VLAN 中去，这样可以很好的控制广播风暴的产生。

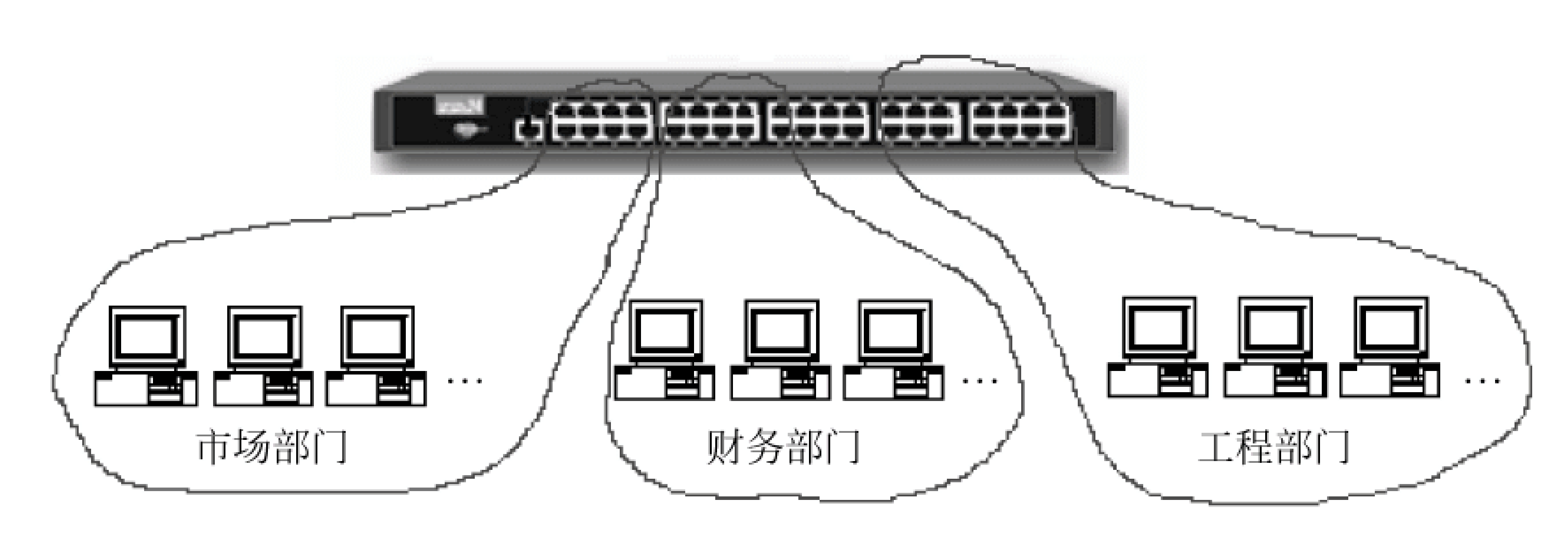


图 3-27 VLAN 示意

需要指出的是，若没有路由的话，不同 VLAN 之间不能相互通信，这样就增加了企业网络中不同部门之间的安全性。由于在局域网上，不同 VLAN 之间的通信数据量是很大的，这样如果路由器要对每一个数据包都路由一次，随着网络上数据量的不断增大，路由器将不堪重负，路由器将成为整个网络的瓶颈。所以在这种情况下，通常采用第三层交换技术。

注意：VLAN 和虚拟专用网（VPN，Virtual Private Network）是截然不同的两个概念。虚拟专用网络能够利用因特网或其他公共因特网络的基础设施为用户创建数据传输隧道，并提供与

专用网络一样的安全和功能保障。VPN是对企业内部网的扩展，通过它可以帮助远程用户、分支机构和商业伙伴建立可信的安全连接。

2. VLAN的分类

1）基于端口划分的VLAN

这是最常应用的一种VLAN，目前绝大多数VLAN协议的交换机都提供这种VLAN配置方法。这种VLAN是根据以太网交换机的交换端口来划分的，它是将VLAN交换机上的物理端口和VLAN交换机内部的PVC（永久虚电路）端口分成若干个组，每个组构成一个虚拟网，相当于一个独立的VLAN交换机。例如，一个交换机的1、2、3、4、5端口被定义为虚拟网A，同一交换机的6、7、8端口组成虚拟网B。这种方法的优点是定义VLAN成员时非常简单，只要将所有的端口都定义为相应的VLAN组即可，适合于任何大小的网络。它的缺点是如果某用户离开了原来的端口，到了一个新的交换机的某个端口，必须重新定义。

2）基于MAC地址划分的VLAN

这种VLAN是根据每个主机的MAC地址来划分，即对每个MAC地址的主机都配置他属于哪个组，VLAN交换机跟踪属于VLAN MAC的地址。这种方式的VLAN允许网络用户从一个物理位置移动到另一个物理位置时，自动保留其所属VLAN的成员身份。

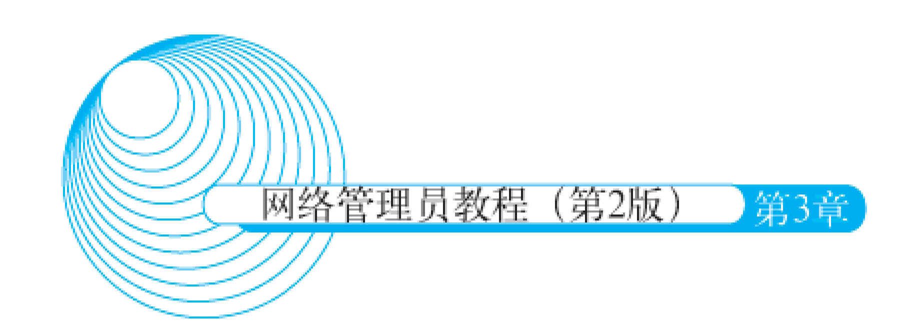
这种VLAN最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN不用重新配置，因为它是基于用户，而不是基于交换机的端口。这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常累的，所以这种划分方法通常适用于小型局域网。而且这种划分的方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个VLAN组的成员，保存了许多用户的MAC地址，查询起来相当不容易。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，这样VLAN就必须经常配置。

3）基于网络层协议划分的VLAN

这种VLAN是根据每个主机的网络层地址或协议类型（如果支持多协议）划分的。VLAN按网络层协议来划分，可分为IP、IPX、DECnet、AppleTalk、Banyan等VLAN网络。虽然这种划分方法是根据网络地址，比如IP地址，但它不是路由，与网络层的路由毫无关系。

这种方法的优点是用户的物理位置改变了，不需要重新配置所属的VLAN，而且可以根据协议类型来划分VLAN。另外，这种方法不需要附加的帧标签来识别VLAN，这样可以减少网络的通信量。

这种方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的（相对于前面两种方法），一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查IP帧头，需要更复杂的技术，同时也更费时。



4）根据 IP 组播划分的 VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN，这种划分的方法将 VLAN 扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展，当然这种方法不适合局域网，主要因为它的效率不高。

3. VLAN 配置实例

下面以 3COM 的 Switch 3300 交换机为例，简单介绍目前最常用的按端口划分 VLAN 的配置方法。假设交换机目前已经通过仿真终端进行了 IP 地址设置。

（1）打开浏览器，在 URL 栏中输入交换机的 IP 地址后按 Enter 键，在 Web 登录界面中输入相应的用户名和密码后，进入 Web 管理页面，单击 configuration 超链接，进入配置页面，然后单击 VLANs 超链接，如图 3-28 所示。

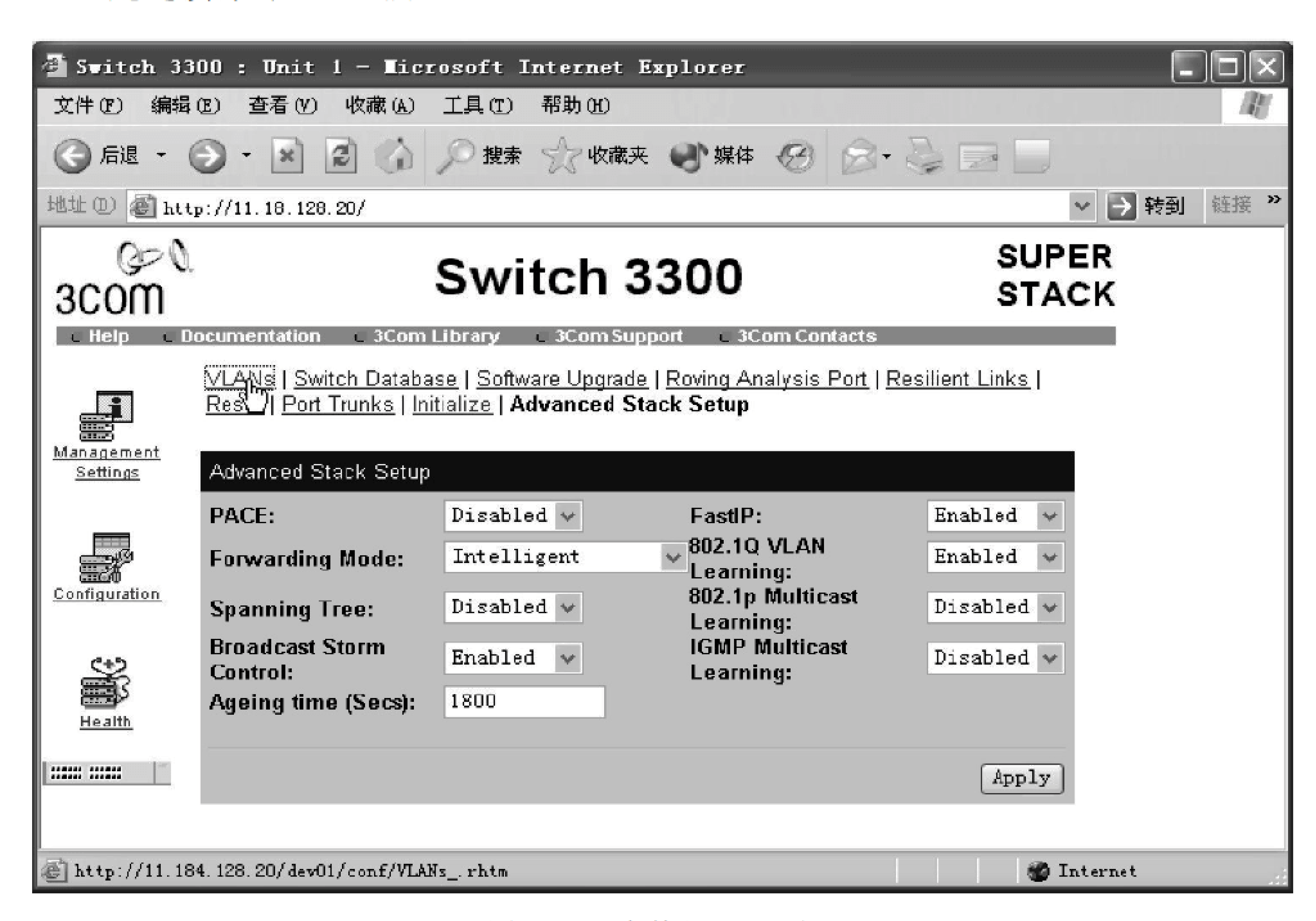


图 3-28　交换机配置页面

（2）在显示的 VLAN 配置页面中单击 Create 按钮，如图 3-29 所示。

（3）在显示的创建 VLAN 名字页面中输入定义的 VLAN 名称。本例中选用了系统自动产生的名称 VLAN 2，如图 3-30 所示。用户定义的 VLAN 之所以从 2 号开始，那是因为每个交换机都有一个默认的 VLAN，那就是 1 号 VLAN，它包括所有连在该交换机上的用户，1 号 VLAN

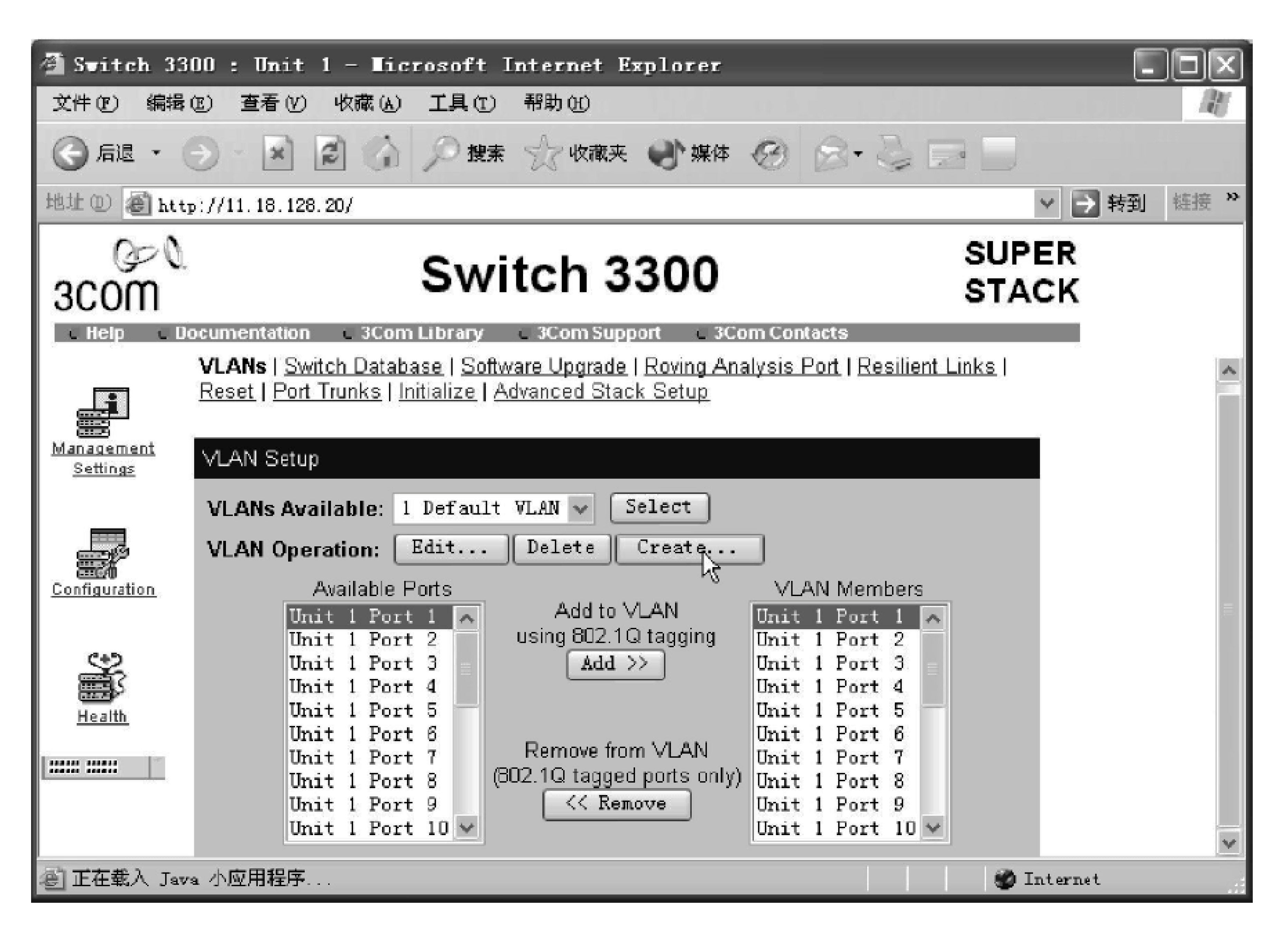


图 3-29　VLAN 配置页面

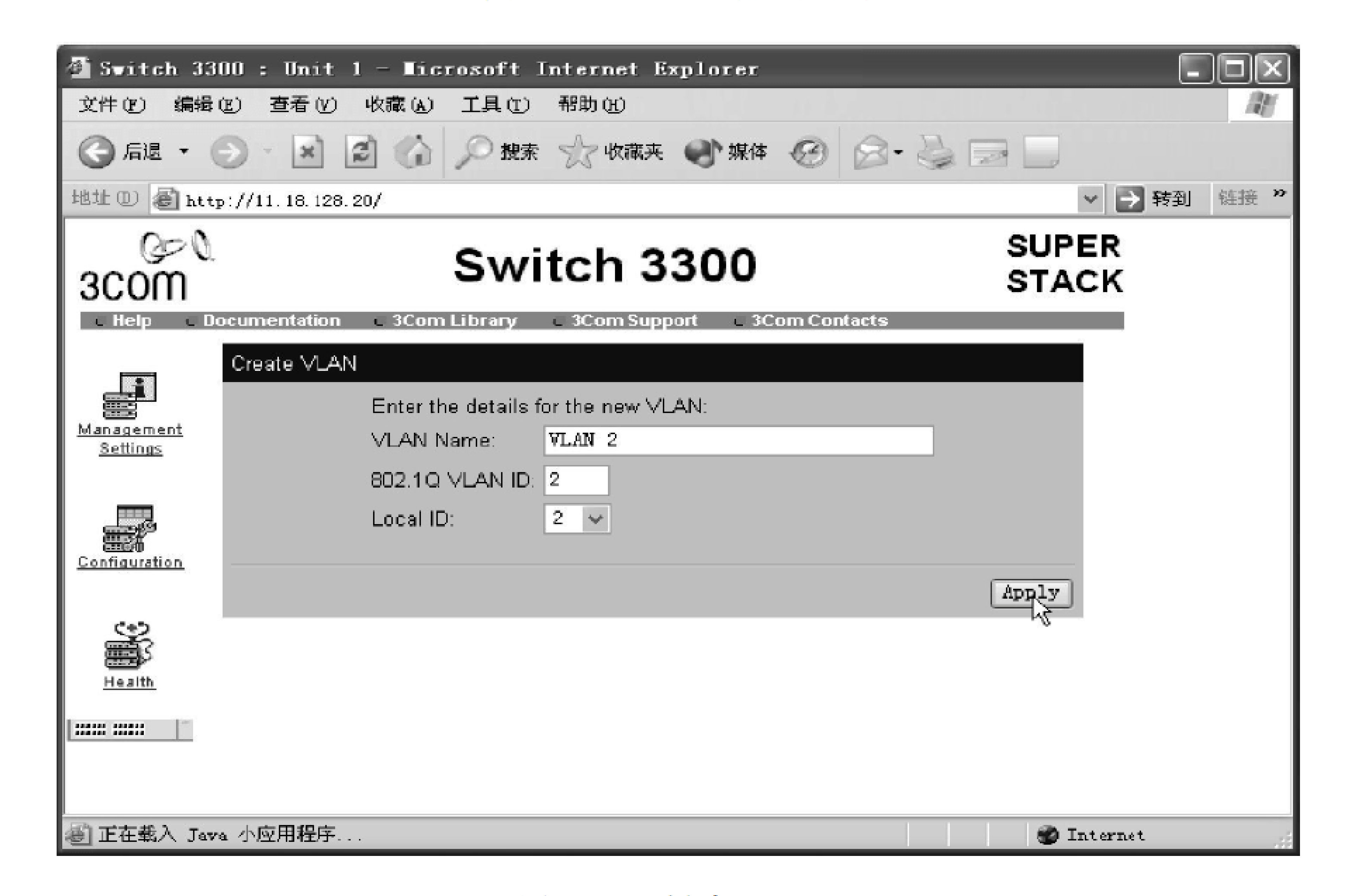


图 3-30　创建 VLAN

是不可以删除的。

（4）在端口分配页面中，依次选定相应的端口，单击 Add 按钮后，相应的端口就被分配到指定的 VLAN 中了，如图 3-31 所示。

（5）重复上述的步骤，再创建其他 VLAN，如图 3-32 所示。当然，用户也可根据自己的喜好，先将所有的 VLAN 都创建好，再依次为各个 VLAN 分配端口。

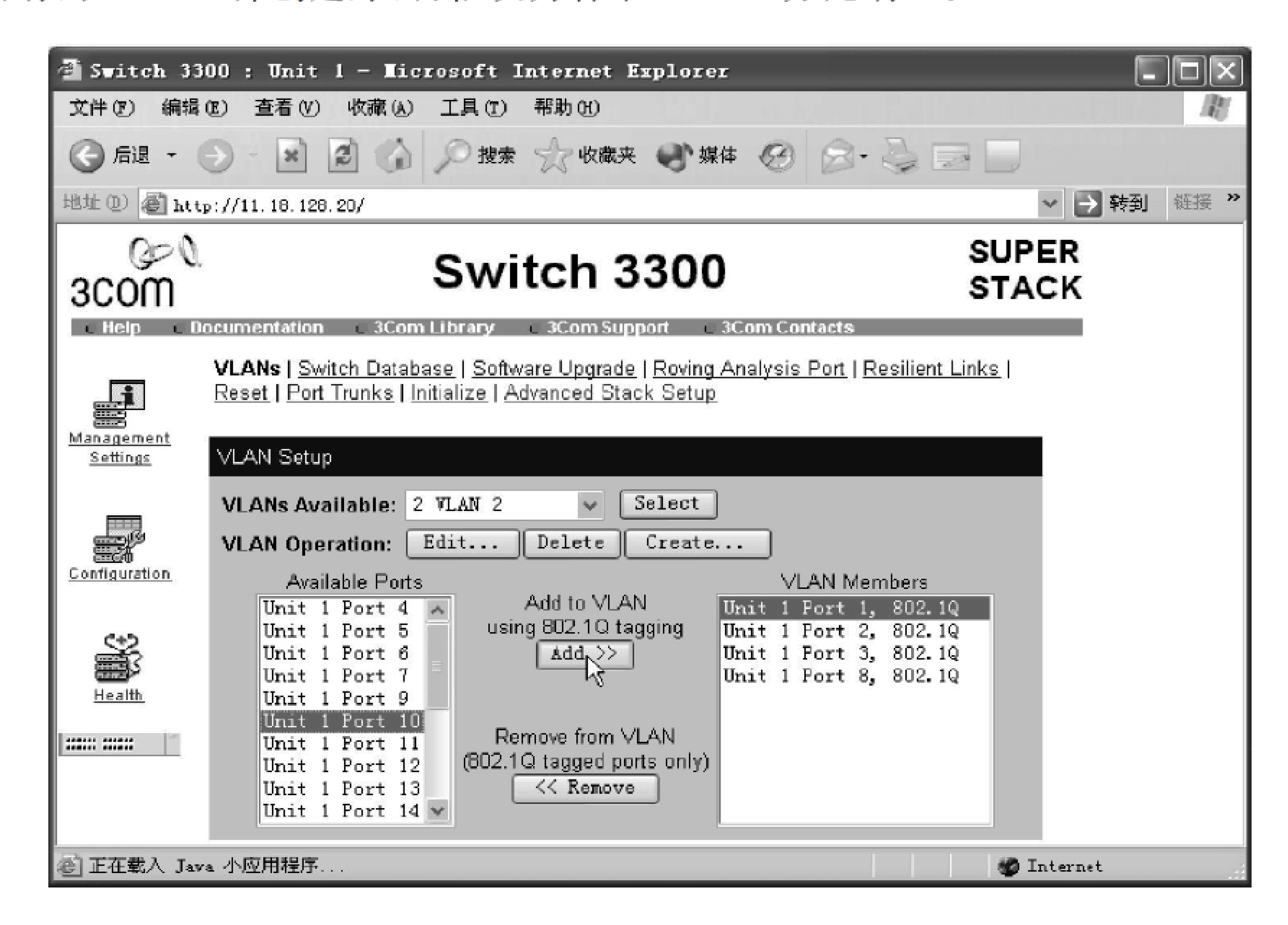


图 3-31　为 VLAN 分配端口

3.2.7　三层交换

1. 三层交换技术的由来

三层交换，又称多层交换或 IP 交换，是将传统交换器与传统路由器结合起来的网络设备，它既可以完成传统交换机的端口交换功能，又可以完成部分路由器的路由功能。

传统的交换技术是在 OSI 参考模型中的第二层（数据链路层）进行操作的，它在操作过程中不断收集信息建立本身的 MAC 地址表。当交换机收到一个以太网帧时，它便会查看该以太网帧的目的 MAC 地址，核对 MAC 地址表以确认该从哪个端口把包发出去。但当交换机收到一个目的地址不在 MAC 地址表中的帧时，交换机便会把该包“扩散”出去，即从所有端口发出去，就如同交换机收到一个广播包一样，这就暴露出传统局域网交换机的弱点：不能有效地隔离广播包，使网络的有效带宽利用率下降，广播包多到一定程度，就有可能形成广播风暴，造成网络

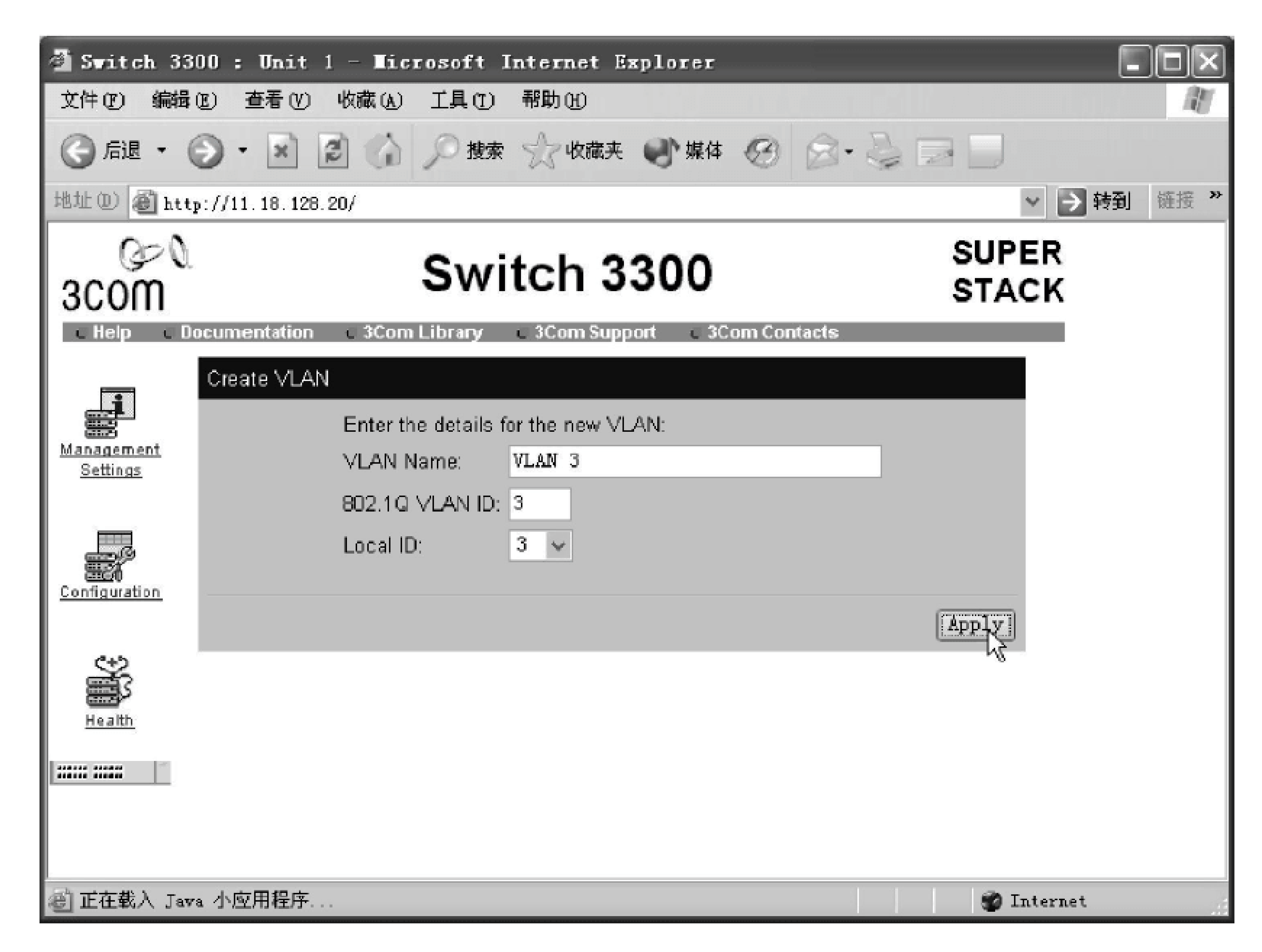
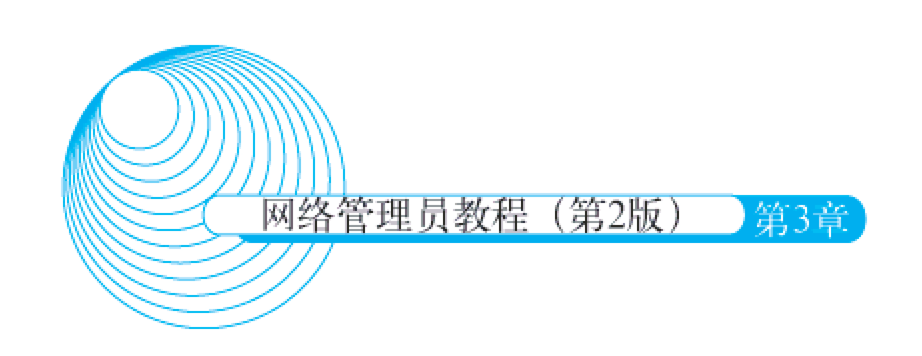


图 3-32　创建下一个 VLAN

瘫痪。因此，产生了交换机上的 VLAN 技术。但是 VLAN 之间的数据传送需要通过路由器实现，路由器成为了网络中的关键设备。

传统的路由技术是在 OSI 参考模型中的第三层（网络层）进行操作的，其核心功能主要包括数据报文转发和路由处理两方面。数据报文转发功能主要是在子网间传送数据报文，包括检查 IP 数据包首部，IP 数据包的分段和重组，修改生存期（TTL）参数，重新计算 IP 数据包的首部检验和，MAC 地址解析等；路由处理子功能包括创建和维护路由表，完成这一功能需要使用路由协议如 RIP 或 OSPF 来建立和形成路由表。路由处理一旦完成，将数据报文发送至目的地址就是报文转发子功能的任务了。传统路由器的弱点是：路由器是一个转发并遗忘的网络设备，对任何数据包都要经过上述复杂的“拆打”过程，即使是同一源地址向同一目的地址发送的数据包，也要重复相同的过程。同时，路由器复杂的处理功能主要是通过软件实现的，也决定了路由器成为局域网通信中不可逾越的瓶颈。

那么，如何有效地解决“在子网间路由时，传输数据仍然采用交换的带宽与速率”呢？三层交换技术应运而生了。三层交换将第二层交换机和第三层路由器的优势结合成为一个有机的整体。三层交换技术的出现，既解决了局域网中网段划分之后网段中的子网必须依赖路由器进行管理的局面，又解决了传统路由器低速、复杂所造成的网络瓶颈问题。简单地说，三层交换技术就是“二层交换＋三层转发”。



2. 三层交换技术的实现

由于三层交换技术不是一种标准化技术，不同厂家的三层交换设备采用了不尽相同的技术实现方法。下面列举几种广泛应用的三层交换技术。

（1）3Com 的 Fast IP：该技术采用了“一次路由，随后交换”的策略，其技术基础是下站解析协议（NHRP，Next Hop Resolution Protocol）。源端主机和目的端主机上都需要运行 Fast IP 协议，交换时，源端主机首先要初始化一个标准的 IP 通信进程，源端主机发送一个 Fast IP 连接请求，该请求就像普通的数据报文一样路由穿过网络，如果目的端主机也运行了 Fast IP 协议，则回传一个包含 MAC 地址的 NHRP 应答，如果二者之间存在交换路径则交换，否则继续路由。

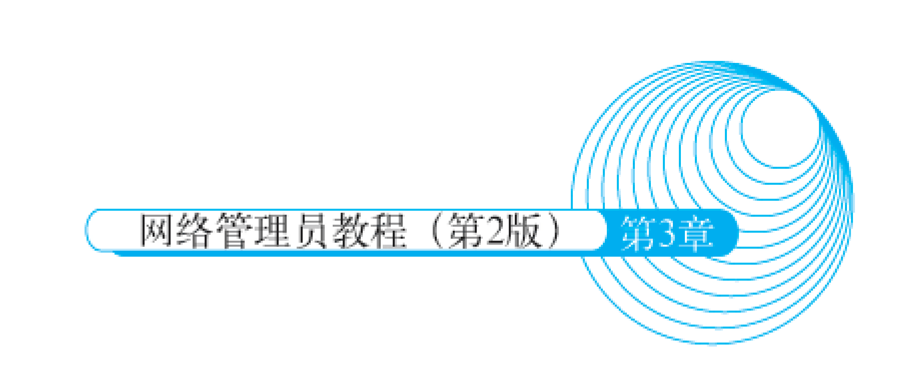
（2）3Com 的 FIRE：被称为灵活智能路由引擎的 FIRE，使用了专用集成电路（ASIC，Application Specific Integrated Circuit）以线速实现第三层的路由和转发，是一个创新的集成化的网间互联体系结构。该技术提供了广泛的第二层和第三层功能，并提供了灵活的网络控制能力，包括网络安全、流量的优化处理、带宽锁定和 QoS 等。

（3）Cisco 的 NetFlow：该技术是对传统的路由转发技术的改进。其基本原理是：第一个数据分组仍然采用传统的第三层路由方式进行转发，转发后第三层交换机把第一个数据分组的信息记录在 NetFlow 的高速缓存中，后继数据分组到达后首先在 Cache 中进行匹配查找，如果命中就使用 Cache 中缓存的路由信息直接转发，否则再进行路由。

（4）Cisco 的标记交换：该技术是在转发时给数据包加上标记。标记是一个较短的长度固定的标号，每个标记可以标识一条或者多条路径的聚集。路由表使用标记进行路由表查找，而不是传统的子网前缀，标记每经过一个路由器就去掉一个域，类似于邮政编码的基本原理。标记的分配是借助标记分配协议（TDP，Tag Distribution Protocol）实现的。

3. 三层交换技术的应用

三层交换从概念的提出到今天的普及应用，虽然只历经了几年的时间，但其在网络建设中的应用越来越广泛。三层交换机以其速度快、性能好、价格低等众多的优势在局域网中已经把路由器排挤到网络的边缘，凡是没有广域网连接需求，同时又需要路由器的地方，都可以用三层交换机代替。正如路由器主宰着广域网一样，三层交换机逐渐走向局域网的统治地位已经是不争的事实。尤其是对于有划分 VLAN 需求的局域网而言，三层交换是最佳选择。三层交换机的典型应用如图 3-33 所示。这是一个三级交换结构的局域网，其中骨干交换机是一台 1000Mbps 三层交换机，支持全双工交换、智能网络管理和多种形式的 VLAN 划分，通过它来划分不同功能的逻辑子网，并通过网络管理系统对整个网络进行集中式控制和管理，包括监控、调整网络的运行状态、统计网上信息流量及用户的使用情况等内容。可直接连到骨干交换机的设备有路由器、各种服务器、中心工作站和二级交换机。二级交换机可选用 100Mbps 的



二层交换机，上行链路接口为1000Mbps，支持VLAN和SNMP。第三级交换机可以选用普通的二层交换机或集线器。

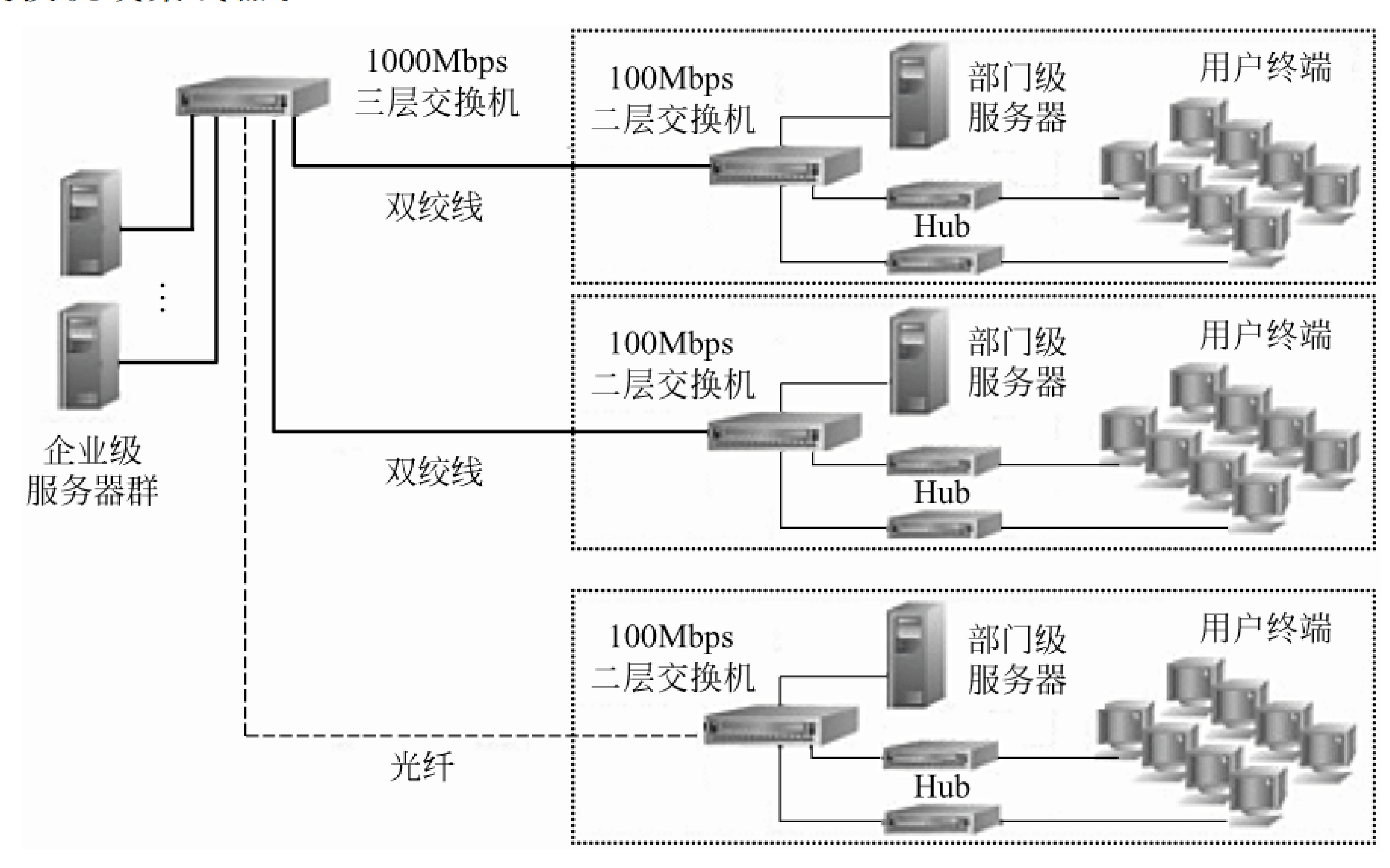


图3-33 三层交换机的典型应用

3.3 综合布线

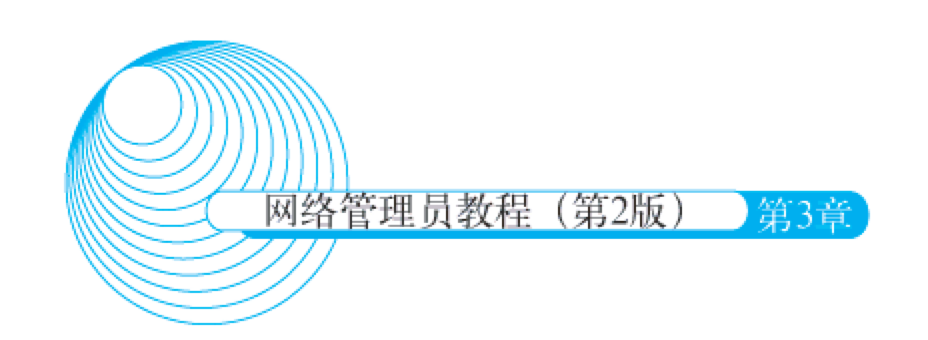
3.3.1 综合布线系统概述

1. 什么是综合布线系统

综合布线系统（PDS，Premises Distribution System），又称结构化综合布线系统（SCS，Structured Cabling System）。综合布线系统是为通信与计算机网络而设计的，它可以满足各种通信与计算机信息传输的要求，是为具有综合业务需求的计算机数据网开发的。综合布线系统具体的应用对象，主要是通信和数据交换，即话音、数据、传真、图影像信号。综合布线系统是一套综合系统，它可以使用相同的线缆、配线端子板、相同的插头及模块插孔，解决传统布线存在的兼容性问题。综合布线系统是建筑智能化大厦工程的重要组成部分，是智能化大厦传送信息的神经中枢。

2. 综合布线系统的特点

综合布线系统是信息技术和信息产业大规模高速发展的产物，是布线系统的一项重大革



新，它和传统布线系统比较，具有明显的优越性，具体表现在以下6个方面：

（1）兼容性。是指其设备可以用于多种系统。沿用传统的布线方式，会使各个系统的布线互不相容，管线拥挤不堪，规格不同，配线插接头型号各异，所构成的网络内的管线与插接件彼此不同而不能互相兼容，一旦要改变终端机或话音设备位置，势必重新敷设新的管线和插接件。而综合布线系统不存在上述问题，它将语音、数据信号的配线统一设计规划，采用统一的传输线、信息插接件等，把不同信号综合到一套标准布线系统中，同时，该系统比传统布线大为简化，不存在重复投资，可以节约大量资金。

（2）开放性。对于传统布线，一旦选定了某种设备，也就选定了布线方式和传输介质，如要更换一种设备，原有布线将全部更换，这样极为麻烦，又增加大量资金。而综合布线系统布线由于采用开放式体系结构，符合国际标准，对现有著名厂商的硬件设备均是开放的，对通信协议也同样是开放的。

（3）灵活性。传统布线各系统是封闭的，体系结构是固定的，若增减设备十分困难。而综合布线系统，如上述所有传递信息线路均为通用的，即每条线路均可传送话音、传真和数据。所用系统内的设备（计算机、终端、网络集散器、集线器或中心集线器、电话、传真）的开通及变动无须改变布线，只要在设备间或管理间作相应的跳线操作即可。

（4）可靠性。传统布线各系统互不兼容，因此在一个建筑物内存在多种布线方式，形成各系统交叉干扰，这样各个系统可靠性降低，势必影响到整个建筑系统的可靠性。综合布线系统布线采用高品质的材料和组合压接方式构成一套标准高的信息网络，所有线缆与器件均通过国际上的各种标准，保证了综合布线系统的电气性能。综合布线系统全部使用物理星型拓扑结构，任何一条线路若有故障不会影响其他线路，从而提高了可靠性，各系统采用同一传输介质，互为备用，又提高了备用冗余。

（5）经济性。综合布线系统设计信息点时要求按规划容量，留有适当的发展容量，因此，就整体布线系统而言，按规划设计所做的经济分析表明，综合布线系统会比传统的价格性能比更优，后期运行维护及管理费也会下降。

（6）先进性。当信息时代快速发展，数据传递和话音传送并驾齐驱，多媒体技术的迅速崛起，如仍采用传统布线，在技术上太落后。综合布线系统采用双绞线与光纤混合布置方式是比较科学和经济的方式。

3. 综合布线标准

综合布线的标准很多，但在实际工程项目中，并不需要涉及所有的标准和规范，而应根据布线项目性质，涉及的相关技术工程情况适当地引用标准规范。通常来说，布线方案设计应遵循布线系统性能和系统设计标准，布线施工工程应遵循布线测试、安装、管理标准及防火、机房及防雷接地标准。

例如，一个典型的办公网络的布线系统集成方案中通常采用的标准如下：

- 《建筑与建筑群综合布线系统工程设计规范》(国家标准 GB30511—2000)；
- 《建筑与建筑群综合布线系统工程施工和验收规范》(国家标准 GB30512—2000)；
- 《大楼通信综合布线系统第一部分总规范》(YD/T 926.1—2001)；
- 《大楼通信综合布线系统第二部分综合布线用电缆光纤技术要求》(YD/T 926.2—2001)；
- 《大楼通信综合布线系统第三部分综合布线用连接硬件技术要求》(YD/T 926.3—2001)；
- 《商用建筑通信布线标准》(北美标准 ANSI/TIA/EIA 568B)；
- 《信息技术——用户通用布线系统》(第二版)(国际标准 ISO/IEC 11801)；
- 《国际电子电气工程师协会:CSMA/CD 接口方法》(IEEE 802.3)。

4. 综合布线系统的构成

综合布线系统由 6 个子系统组成，即建筑群子系统、设备间子系统、干线子系统、管理子系统、配线子系统、工作区子系统。大型布线系统需要用铜介质和光纤介质部件将六个子系统集成在一起。综合布线 6 个子系统的构成如图 3-34 所示。

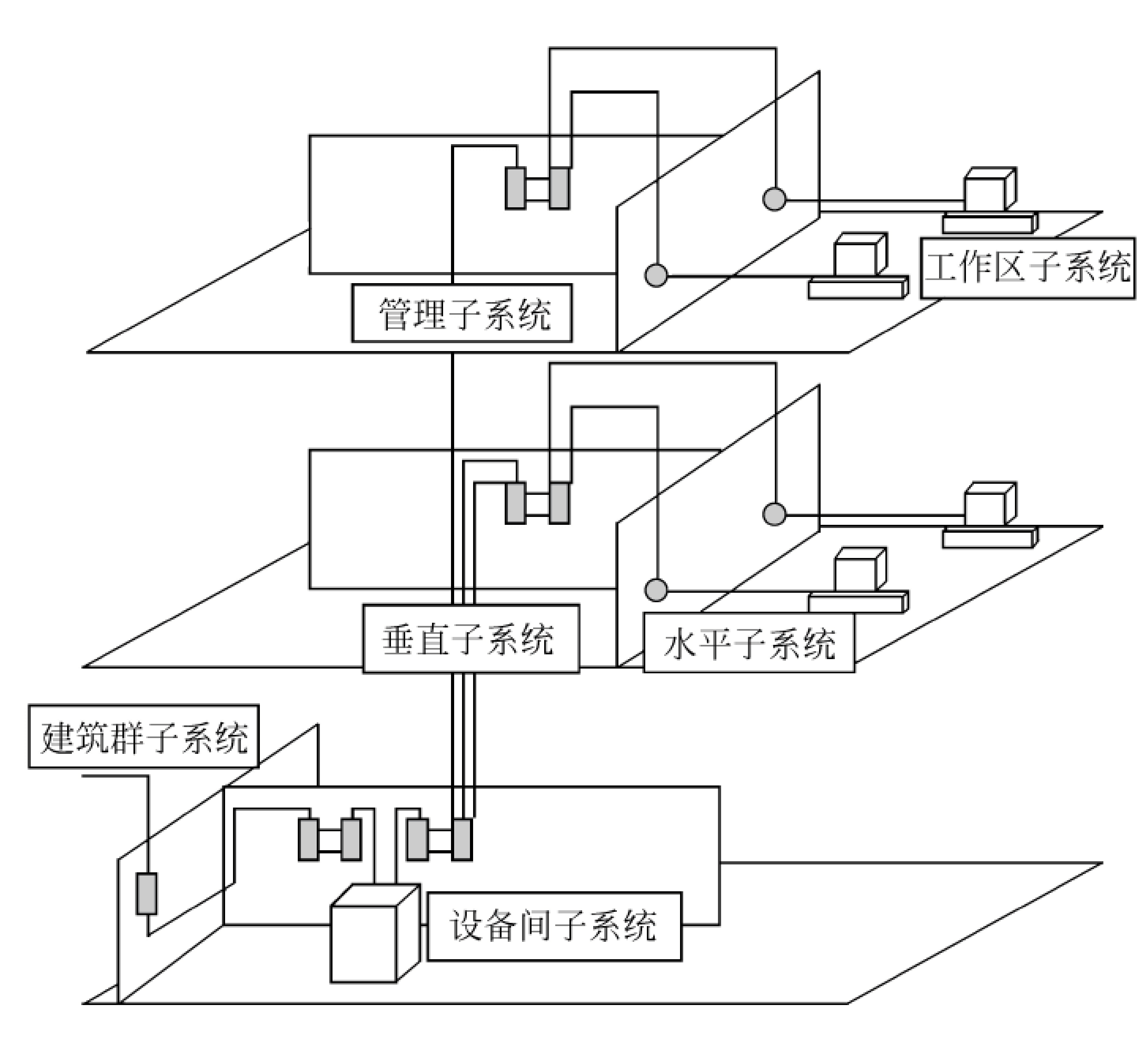
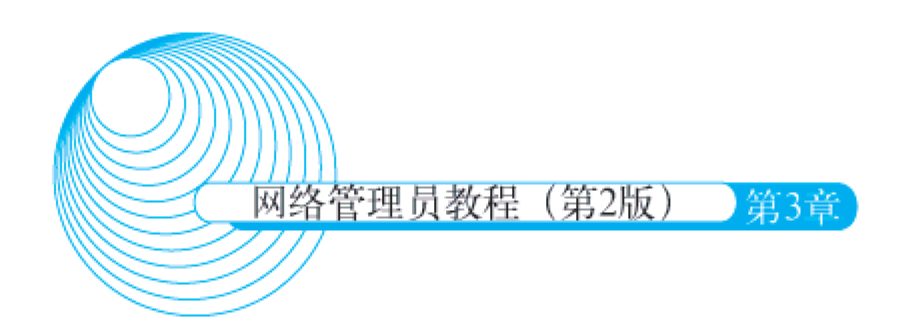


图 3-34 综合布线系统的构成

(1) 水平子系统(Horizontal Subsystem)：由信息插座、配线电缆或光纤、配线设备和跳线等组成，又称之为配线子系统。



(2) 垂直子系统(Backbone Subsystem):由配线设备、干线电缆或光纤、跳线等组成，又称之为干线子系统。

(3) 工作区子系统(Work Area Subsystem):为需要设置终端设备的独立区域。

(4) 管理子系统(Administration Subsystem):是针对设备间、交接间、工作区的配线设备、缆线、信息插座等设施进行管理的系统。

(5) 设备间子系统(Equipment Room Subsystem):是安装各种设备的场所，对综合布线而言，还包括安装的配线设备。

(6) 建筑群子系统(Campus Subsystem):由配线设备、建筑物之间的干线电缆或光纤、跳线等组成。

3.3.2 综合布线系统设计

1. 系统设计原则

与其他系统设计一样，设计者首先要进行用户需求分析，然后根据需求分析进行方案设计。但需要指出的是，综合布线系统理论上讲可以容纳：话音，包括电话、传真、音响(广播)；数据，包括计算机信号、公共数据信息；图像，包括各种电视信号、监视信号；控制信号，包括温度、压力、流量、水位以及烟雾等各类控制信号。但实际工程中，至少在目前技术条件和工程实际需要中多为前两种话音和数据，原因是多方面的，其中值得注意的是：话音的末端装置和计算机网络的终端用户装置往往是要变动的，有的是经常变动的，因此采用综合布线系统及其跳选功能，很容易在不改动原有的敷线条件下满足用户的需求。此外，本来可用同轴电缆可靠地传输电视信号，若改用综合布线，则要增设昂贵的转换器。对消防报警信号用普通双绞线已达到要求，若改用综合布线，经过配线架再次终接，也无此必要。因此集成化的要求应视实际需要来定。

在进行综合布线系统设计时通常应遵循以下原则：

(1) 采用模块化设计，易于在配线上扩充和重新组合；

(2) 采用星型拓扑结构，使系统扩充和故障分析变得十分简易；

(3) 应满足通信自动化与办公自动化的需要，即满足话音与数据网络的广泛要求；

(4) 确保任何插座互连主网络，尽量提供多个冗余互连信息点插座；

(5) 适应各种符合标准的品牌设备互连入网，满足当前和将来网络的要求；

(6) 电缆的敷设与管理应符合综合布线系统设计要求。

2. 工作区子系统设计

根据综合布线设计规范的工程经验，并结合用户的实际建筑情况，除去走廊、过道等因素，考虑建筑面积的70%为实际办公面积，办公区每8～10m^{2}一个双孔信息出口，可配一部电话，一

部计算机。信息插座通常可有3种安装形式：

(1) 信息插座安装于地面上。要求安装于地面的金属底盒应当是密封的、防水、防尘并可带有升降的功能。此方法设计安装造价较高，并且由于事先无法预知工作人员的办公位置，也不知分隔板的确切位置，因此灵活性不是很好。

(2) 信息插座安装于分隔板上。此方法适于分隔板位置确定以后，安装造价较为便宜。

(3) 信息插座安装于墙上。此方法在分隔板位置未确定情况下，可沿大开间四周的墙面每隔一定距离均匀地安装RJ45埋入式插座。此方法和前两种方式相比，无论在系统造价、移动分隔板的方便性、整洁度，还是在安装和维护方面都是很好的。

标准信息插座，型号为RJ45，采用8芯接线，全部按标准制造，符合ISDN标准。通常数据和语音均采用MDVO(多媒体信息)模块式超5类信息插座。在RJ45插座内不仅可以插入数据通信通用的RJ45接头，也可以插入电话机专用的RJ12插头。

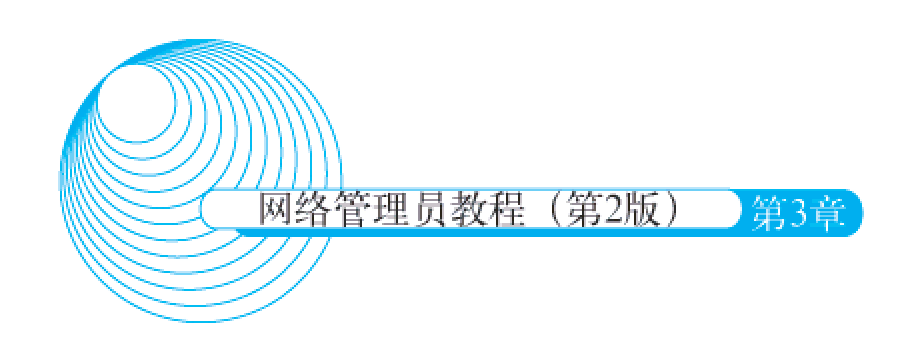
3. 水平子系统设计

水平子系统是将垂直子系统线路延伸到用户工作区，由工作区的信息插座、信息插座至楼层配线设备(FD)的配线电缆或光纤、楼层配线设备和跳线等组成。该系统是从各个子配架子系统出发连向各个工作区的信息插座。水平子系统要求走廊的吊顶上应安装有金属线槽，进入房间时，从线槽引出金属管以埋入方式由墙壁而下到各个信息点。通常水平子系统采用双绞线，在需要时也可采用光纤，根据整个综合布线系统的要求，应在交换间或设备间的配线设备上进行连接。如果采用双绞线，长度不应超过90m。在保证链路性能的情况下，水平光纤距离可适当加长。信息插座采用8位模块式通用插座或光纤插座。配线设备交叉连接的跳线应选用综合布线专用的软跳线，在电话应用时也可选用双芯跳线。

双绞线作为水平子系统的主要组成部分，通常采用管线敷设，一般应使用20年左右，这也对双绞线的性能和质量提出了更高的要求。所以，应根据具体网络工程，合理选择双绞线。比较好的办法是：从实际应用出发，考虑未来发展的余地和投资费用，确保安装质量。从实际出发是指要考虑目前用户对网络应用的要求有多高，100Mbps以太网是否够用。因为网络的布线系统是一次性长期投资，考虑未来发展是指要考虑到网络的应用是否在一段时期内会有对千兆以太网或未来更高速的网络的需求。

就目前而言，进行一个新工程的永久性的综合布线，通常需要在超5类和6类之间选择。超5类系统可以支持千兆以太网的运行，而且不同厂商的超5类系统之间可以互用。6类价格较之超5类昂贵，但其带宽却由200MHz扩大到250MHz，提高了25%，显示了传输速率的增强。目前，6类双绞线已经在少数工程中超前采用。

注意：6类系统是专用的，元件的指标仍在研究之中。各个厂商的元器件都有独特的设计和性能指标，互通的可能性很小。



4. 垂直子系统设计

垂直子系统主要用于连接各层配线室，并连接主配线室。垂直子系统要求建筑物竖井中应立有金属线槽，且每隔两米焊一根粗钢筋，以安装和固定垂直子系统的电缆。竖井中的线槽应和各层配线室之间有金属线槽连通。

垂直子系统实现计算机设备、程控交换机(PBX)、控制中心与各管理子系统间的连接，常用介质是大对数双绞线电缆、光纤。垂直干线部分提供了建筑物中主配线架与分配线架连接的路由，通常采用 IBDNPLUS 型、ATMM 或 DFlex 型大对数铜缆和 62.5/125μm 多模光纤来实现这种连接。

ATMM、DFlex 属于大对数 3 类双绞线，通常被用作电话及广播信号等低速率的主干传输线缆。IBDN PLUS 型大对数电缆属于超 5 类的传输介质，其特性与水平子系统所用的同类线材的物理特性相同，被用作计算机、视频图像等高速数据应用的主干传输线缆。

多模光纤的优点为：光耦合率高，纤芯对准要求相对较宽松。当弯曲半径大于其直径 20 倍时不影响信号的传输，是符合 IEEE 802.5 FDDI 和 EIA/TIA568 标准的光传输介质。用于计算机数据传输距离超过 100m 时的应用，其传输距离可达 2km。在保密性要求高的场合，建议也采用光纤传输。对于距离强电磁干扰源较近的情况，亦需要利用光纤的抗干扰性好的优点。充分考虑到投资的回报率和性能价格比，一般情况下语音干缆采用符合 EIA/TIA568 标准的大对数 3 类双绞线，数据干缆采用 NTF－CMGR－06 多模光纤。

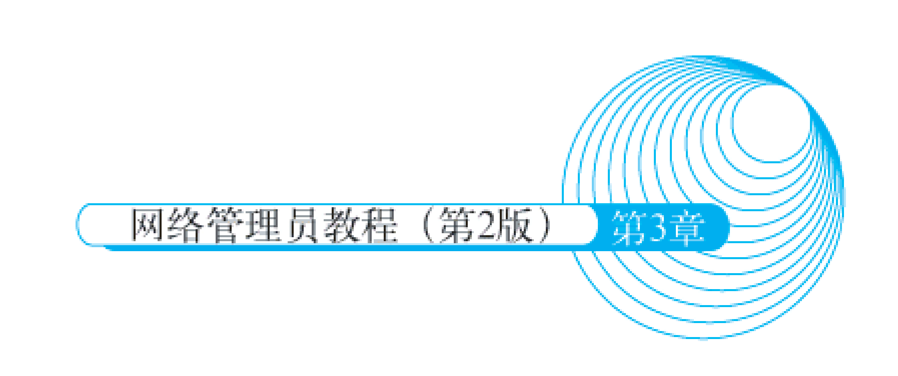
5. 管理子系统设计

管理子系统由交连、互连配线架组成，为连接其他子系统提供连接手段。交连和互连允许将通信线路定位或重定位到建筑物的不同部分，以便能更容易地管理通信线路，并且在移动终端设备时能方便地进行插拔。分配线间是各管理子系统的安装场所。

分配线间可位于大楼的某一层或以多层共用一个配线间的方式分布，用于将连接至工作区的水平线缆与自设备间引出的垂直线缆相连接。

对于信息点不是很多，使用功能又近似的楼层，为便于管理，可共用一个子配线间；对于信息点较多的楼层应在该层设立配线室。配线室的位置可选在弱电竖井附近的房间内。配线室用于安装配线架和安装计算机网络通信设备。

通常管理子系统使用墙装式光纤接续装置(光纤配线架)，置于各层的配线间内。其上嵌 1 块 6ST 耦合器面板，ST 接头由陶瓷材料制成，最大信号衰减量小于 0.2dB。光纤接续装置将自设备间引出的光纤引入，通过光纤跳线与网络设备相连，由网络设备上的 UTP 端口经 UTP 跳线与配线架(置于 19 英寸机柜中)相连。



6. 设备间子系统设计

设备间子系统(主配线间)由设备间中的电缆、连接器和相关支撑硬件组成,它把公共系统设备的各种不同设备互连起来。该子系统将中继线交叉连接处和布线交叉处与公共系统设备(如 PBX)连接起来。

通常主配线架设置在程控机房内,用于垂直干缆和 PABX 的连接,建议采用 QCBIX 系列配线架,可充分满足话音通信的要求。通常计算机网络主配线架设在网管中心,使用光纤配线架,用来端接来自各分配线间的光纤,并通过光纤跳线和计算机网络中心交换机相连。光纤配线架采用 24/48 口配线箱,适用于光纤数量多密度大的场合。可直接安装在标准的 19 英寸机柜内,用于主干光纤和网络设备的连接,十分易于管理。

按照标准的设计要求,设备间尤其是要集中放置设备的设备间,应尽量满足下面的要求:

(1) 将服务电梯安排在设备间附近,以便装运笨重的设备;

(2) 室温应保持在 18～27℃,相对湿度保持在 30%～55%;

(3) 保持室内无尘或少尘,通风良好,亮度至少达 30lx;

(4) 安装合适的消防系统(如采用湿型消防系统,不要把喷头直接对准电气设备);使用防火门,至少能耐火 1 小时的防火墙和阻燃漆;

(5) 提供合适的门锁,至少要有一扇窗口留作安全出口;

(6) 尽量远离存放危险物品的场所和电磁干扰源(如发射机和电动机);

(7) 设备间的地板负重能力至少应为 $500kg/m^2$;

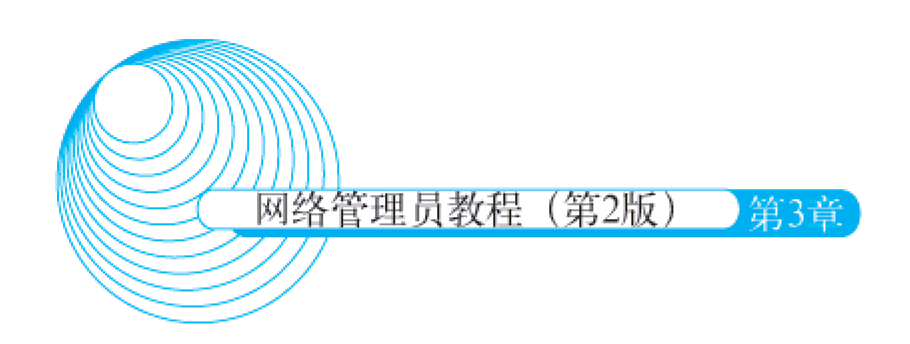
(8) 标准的天花板高度为 240cm,门的大小至少为 210cm×150cm,向外开;

(9) 在设备间尽量将设备机柜放在靠近竖井的位置,在柜子上方应装有通风口用于设备通风;

(10) 在配线间内应至少留有两个专用的 220V/10A 单相三极电源插座。如果需要在配线间内放置网络设备,则还应根据放置设备的供电需求,配有另外的 220V/10A 专用线路,此线路不应与其他大型设备并联,并且最好先连接到 UPS,以确保对设备的供电及电源的质量。

7. 建筑群子系统设计

建筑群子系统应由连接各建筑物之间的综合布线缆线、建筑群配线设备(CD)和跳线等组成。建筑物之间的缆线宜采用地下管道或电缆沟的敷设方式。建筑物群干线电缆、光纤、公用网和专用网电缆、光纤(包括天线馈线)进入建筑物时,都应设置引入设备,并在适当位置终端转换为室内电缆、光纤。引入设备还包括必要的保护装置。引入设备宜单独设置房间,如条件合适也可与 BD 或 CD 合设。建筑群和建筑物的干线电缆、主干光纤布线的交接不应多于两次。从楼层配线架(FD)到建筑群配线架(CD)之间只应通过一个建筑物配线架(BD)。



8. 管线设计

在综合布线系统中管线设计通常有两种方案，一种是用于墙上型信息出口的采用走吊顶的装配式槽形电缆桥架的方案。这种方式适用于大型建筑物，为水平线系统提供机械保护和支持；另一种是用于地面型信息出口的地面线槽走线方式。这种方式适用于大开间的办公间，有大量地面型信息出口的情况。

1）装配式槽形电缆桥架

装配式槽形电缆桥架是一种闭合式的金属托架，安装在吊顶内，从弱电井引向各个设有信息点的房间，再由预埋在墙内的不同规格的铁管，将线路引到墙上的暗装铁盒内。

线槽的材料为冷轧合金板，表面可进行相应处理，如镀锌、喷塑、烤漆等。线槽可以根据情况选用不同的规格。为保证线缆的转弯半径，线槽须配以相应规格的分支辅件，以确保线路的弯转自如。

同时为确保线路的安全，应使槽体有良好的接地端。金属线槽、金属软管、电缆桥架及各分配线箱均需整体连接，然后接地。如果不能确定信息出口的准确位置，拉线时可先将线缆盘在吊顶内的出线口，待具体位置确定后，再引到各信息出口。

2）地面线槽走线

地面线槽走线方式通常先在地面垫层中预埋金属线槽，主线槽从弱电井引出，沿走廊引向各方向，到达设有信息点的各房间时，再用支线槽引向房间内的各信息点出线口。强电线路可以与弱电线路平行配置，但需分隔于不同的线槽中。这样可以向每一个用户提供一个包括数据、语音、不间断电源、照明电源出口的集成面板。真正地做到在一个清洁的环境下，实现办公室自动化。

由于地面垫层中可能会有消防等其他系统的线路，所以必须与由建筑设计单位和建筑施工单位一起，综合各系统的实际情况，完成地面线槽路由部分的设计。另外，地面线槽也需整体连接，然后接地。

按照标准的线槽设计方法，应根据水平线的外径来确定线槽的横截面积，即：

线槽的横截面积＝水平线截面积之和×3

9. 电气防护、接地及防火设计

综合布线系统应根据环境条件选用相应的缆线和配线设备，或采取防护措施，并应符合下列规定：

(1) 当综合布线区域内存在干扰或用户对电磁兼容性有较高要求时，宜采用屏蔽缆线和屏蔽配线设备进行布线，也可采用光纤系统。采用屏蔽布线系统时，所有屏蔽层应保持连续性。

(2) 综合布线系统采用屏蔽措施时，必须有良好的接地系统。保护地线的接地电阻值，单独设置接地体时，不应大于4Ω；采用接地体时，不应大于1Ω。采用屏蔽布线系统时，屏蔽层的配线设备(FD或BD)端必须良好接地，用户(终端设备)端视具体情况接地，两端的接地应连接至同一接地体。若接地系统中存在两个不同的接地体时，其接地电位差不应大于1Vr.m.s(voltage

root. mean. square，电压有效值）。每一楼层的配线柜都应采用适当截面的铜导线单独布线至接地体，也可采用竖井内集中用铜排或粗铜线引到接地体，导线或铜导体的截面应符合标准。接地导线应接成树状结构的接地网，避免构成直流环路。

（3）当电缆从建筑物外面进入建筑物时，电缆的金属护套或光纤的金属件均应有良好的接地，同时要采用过压，过流保护措施，并符合相关规定。

（4）根据建筑物的防火等级和对材料的耐火要求，综合布线应采取相应的措施。在易燃的区域和大楼竖井内布放电缆或光纤，应采用阻燃的电缆和光纤；在大型公共场所宜采用阻燃、低燃、低毒的电缆或光纤；相邻的设备间或交换间应采用阻燃型配线设备。

（5）当综合布线路由上存在干扰源，且不能满足最小净距要求时，宜采用金属管线进行屏蔽。综合布线电缆与附近可能产生高频电磁干扰的电动机、电力变压器等电气设备之间应保持必要的间距。综合布线电缆与电力电缆的间距应符合表 3-2 的规定。墙上敷设的综合布线电缆、光纤及管线与其他管线的间距应符合表 3-3 的规定。

表 3-2　综合布线电缆与电力电缆的间距

类　别	与综合布线接近状况	最小净距（mm）
380V 电力电缆 <2kW	与缆线平行敷设	130
	有一方在接地的金属线槽或钢管中	70
	双方都在接地的金属线槽或钢管中	10
380V 电力电缆 2～5kW	与缆线平行敷设	300
	有一方在接地的金属线槽或钢管中	150
	双方都在接地的金属线槽或钢管中	80
380V 电力电缆 >5kW	与缆线平行敷设	600
	有一方在接地的金属线槽或钢管中	300
	双方都在接地的金属线槽钢管中	150

表 3-3　墙上敷设的综合布线电缆、光纤及管线与其他管线的间距

其他管线	电缆、光纤或管线与其他管线的间距	
	最小平行净距（mm）	最小交叉净距（mm）
避雷引下线	1000	300
保护地线	50	20
给水管	150	20
压缩空气管	150	20
热力管（不包封）	500	500
热力管（包封）	300	300
煤气管	300	20

3.3.3 综合布线系统的性能指标及测试

综合布线作为网络中最基本、最重要的组成部分，是连接每台服务器和工作站的纽带。作为传输高速数据的介质，综合布线系统对线缆的要求较严格，一旦线缆产生故障，严重时可导致整个网络系统的瘫痪。一个布线系统的传输性能是由多种因素决定的：线缆特性、连接硬件、跳线、整体回路连接数目以及设计和安装质量。即使线缆和连接硬件都符合国际标准，但由于在布线系统的设计和安装过程中加入了许多人为因素，必须对整个布线系统进行全面测试，以证明布线系统的安装是合格的。

1. 双绞线系统的测试元素及标准

通常，双绞线系统的测试指标主要集中在链路传输的最大衰减值和近端串音衰减等参数上。链路传输的最大衰减值是由于集肤效应、绝缘损耗、阻抗不匹配、连接电阻等因素，造成信号沿链路传输损失的能量。电磁波从一个传输回路（主串回路）串入另一个传输回路（被串回路）的现象称为串音，能量从主串回路串入回路时的衰减程度称为串音衰减。在 UTP 布线系统中，近端串音为主要的影响因素。

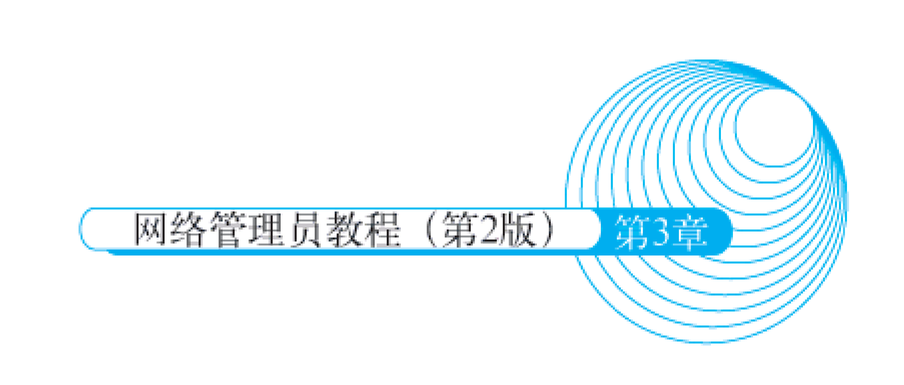
下面给出双绞线系统的几个主要测试元素及标准。需要指出的是，表中数值为通道回路总长度为 100m 以内、基本回路总长度为 94m 以内、测试温度为 20℃下的标准值。

1）链路传输的最大衰减限值

综合布线系统链路传输的最大衰减限值，包括配线电缆和两端的连接硬件、跳线在内，应符合表 3-4 的规定。

表 3-4　链路传输的最大衰减限值

频率（MHz）	最大衰减值（dB）			
	A 级	B 级	C 级	D 级
0.1	16	5.5		
1.0		5.8	3.7	2.5
4.0			6.6	4.8
10.0			10.7	7.5
16.0			14.0	9.4
20.0				10.5
31.25				13.1
62.5				18.4
100.0				23.2



2）近端串音(NEXT)衰减限值

综合布线系统任意两线之间的近端串音衰减限值，包括配线电缆和两端的连接硬件、跳线、设备和工作区连接电缆在内(但不包括设备连接器)，应符合表 3-5 的规定。

表 3-5　线对间最小近端串音衰减限值

频率(MHz)	最大衰减值(dB)			
	A 级	B 级	C 级	D 级
0.1	27	40		
1.0		25	39	54
4.0			29	45
10.0			23	39
16.0			19	36
20.0				35
31.25				32
62.5				27
100.0				24

3）回波损耗限值

综合布线系统中任一电缆接口处的回波损耗限值，应符合表 3-6 的规定。

表 3-6　电缆接口处最小回波损耗限值

频率(MHz)	最小回波损耗值	
	C 级	D 级
10≤f<16	15	15
16≤f<20		15
20≤f<100		10

2．光纤布线系统的测试元素及标准

由于在光纤系统的实施过程中，涉及到光纤的镉铺设，光纤的弯曲半径，光纤的熔接、跳线，更由于设计方法及物理布线结构的不同，导致两网络设备间的光纤路径上光信号的传输衰减有很大不同。虽然光纤的种类较多，但光纤及其传输系统的基本测试方法大体相同，所使用的测试仪器也基本相同。对磨接后的光纤或光纤传输系统，必须进行光纤特性测试，使之符合光纤

传输通道测试标准。基本的测试内容包括：

1）波长窗口参数

综合布线系统光纤波长窗口的各项参数，应符合表 3-7 的规定。

表 3-7　光纤波长窗口参数

光纤模式	波长下限(nm)	波长上限(nm)	基准试验波长(nm)	谱线最大宽度(nm)
多模	790	910	850	50
多模	1285	1330	1300	150
单模	1288	1339	1310	10
单模	1525	1575	1550	10

2）光纤布线链路的最大衰减限值

综合布线系统的光纤布线链路的衰减限值，应符合表 3-8 的规定。

表 3-8　光纤布线链路的最大衰减限值

应用类别	链路长度(m)	多模衰减值(dB)		单模衰减值(dB)	
		850nm 波长	1300nm 波长	1310nm 波长	1550nm 波长
水平子系统	100	2.5	2.2	2.2	2.2
垂直子系统	500	3.9	2.6	2.7	2.7
建筑群子系统	1500	7.4	3.6	3.6	3.6

3）光回波损耗限值

综合布线系统光纤布线链路任一接口的光回波损耗限值，应符合表 3-9 的规定。

表 3-9　最小的光回波损耗限值

光纤模式	标称波长(nm)	最小的光回波损耗限值(dB)
多模	850	20
多模	1300	20
单模	1310	26
单模	1550	26

3．测试环境

为了保证布线系统测试数据准确可靠，对测试环境有着严格的规定。

1）测试条件

综合布线最小模式带宽测试现场应无产生严重电火花的电焊、电钻和产生强磁干扰的设备作业，被测综合布线系统必须是无源网络、无源通信设备。

2）测试温度

综合布线测试现场温度在20～30℃之间，湿度宜在30%～80%，由于衰减指标的测试受测试环境温度影响较大，当测试环境温度超出上述范围时，需要按照有关规定对测试标准和测试数据进行修正。

3）测试仪表

按时域原理设计的测试仪均可用于综合布线现场测试，但测试仪的测量扫描步长要满足近端串扰指标测量精度的基本保证，能够在0～250MHz频率范围内提供各测试参数的标称值和阈值曲线，每测试一条链路时间不应大于25s，且每条链路应具有一定的故障定位诊断能力，具有自动、连续、单项选择测试的功能。

4. 测试流程

在开始测试之前，应该认真了解布线系统的特点、用途，信息点的分布情况，确定测试标准，选定测试仪后按以下程序进行：

（1）测试仪测试前自检，确认仪表是正常的；

（2）选择测试了解方式；

（3）选择设置线缆类型及测试标准；

（4）NVP值核准，核准NVP使用缆长不短于15m；

（5）设置测试环境湿度；

（6）根据要求选择“自动测试”或“单项测试”；

（7）测试后存储数据并打印；

（8）发生问题修复后复测；

（9）测试中出现“失败”查找故障。

第4章　网络操作系统

4.1　网络操作系统概述

4.1.1　什么是网络操作系统

1. 网络操作系统的概念

网络操作系统(NOS,Network Operation System),首先它必须是一个操作系统。那么什么是操作系统呢？一个完整的计算机系统是由硬件系统和软件系统两大部分组成的。仅有硬件,计算机是不能自行工作的,还必须给它配备“思想”,即指挥它如何工作的软件。软件家族中最重要的系统软件就是操作系统,它有两个功能:一是管理计算机系统的各种软、硬件资源。那么多的软件、硬件资源组合在一起,如何才能有条不紊地工作呢？靠的就是操作系统的管理,由操作系统对资源进行统一分配、协调。二是提供人机交互的界面。在计算机内部,处理和存储的都是二进制数据,人是不能直接识别的,人对计算机下达的命令,计算机也是不能识别的,为此,中间需要一个翻译,这个翻译就是操作系统。

网络操作系统作为一个操作系统也应具有上述功能,以实现网络中的资源管理和共享。计算机单机操作系统是用户和计算机之间的接口,网络操作系统则是网络用户和计算机网络之间的接口。计算机网络不只是计算机系统的简单连接,还必须有网络操作系统的支持。网络操作系统的任务就是支持网络的通信及资源共享,网络用户则通过网络操作系统请求网络服务。而网络操作系统除了具备单机操作系统所需的功能如:处理器管理、存储器管理、设备管理和文件管理等功能之外,还必须承担整个网络范围内的任务管理以及资源的管理与分配任务,能够对网络中的设备进行存取访问,能够提供高效可靠的网络通信能力,提供更高一级的服务。除此之外,它还必须兼顾网络协议,为协议的实现创造条件和提供支持。

简单地讲,网络操作系统是使联网计算机能够方便而有效地共享网络资源,为网络用户提供所需的各种服务的软件与协议的集合。网络操作系统是网络的心脏和灵魂,是向网络计算机提供服务的特殊的操作系统,它在计算机操作系统下工作,使计算机操作系统增加了网络操作所需要的能力。

2. 网络操作系统的功能

网络操作系统的基本功能有:

(1) 文件服务;

（2）打印服务；
（3）数据库服务；
（4）通信服务；
（5）信息服务；
（6）分布式服务；
（7）网络管理服务；
（8）Internet/Intranet 服务。

3. 网络操作系统的特点

作为网络用户和计算机网络之间的接口，一个典型的网络操作系统一般具有以下特点：

（1）具有复杂性。单机操作系统的主要功能是管理本机的软硬件资源，而网络操作系统一方面要对全网资源进行管理，以实现整个网络的资源共享。另一方面，还要负责计算机间的通信与同步。显然比单机操作系统要复杂得多。

（2）具有并行性。单机操作系统通过为用户建立虚拟处理器来模拟多机环境，从而实现程序的并发执行。而网络操作系统在每个节点上的程序都可以并发执行，一个用户作业既可以在本地运行，也可以在远程节点上运行。在本地运行时，还可以分配到多个处理器中并行操作。

（3）具有高效性。网络操作系统中采用多线程的处理方式。线程相对于进程而言需要较少的系统开销，比进程更易于进行管理。采用抢先式多任务时，操作系统不用专门等待某一线程的完成后，再将系统控制交给其他线程，而是主动将系统控制交给首先申请得到系统资源的其他线程，这样就可以使系统运行具有更高的效率。

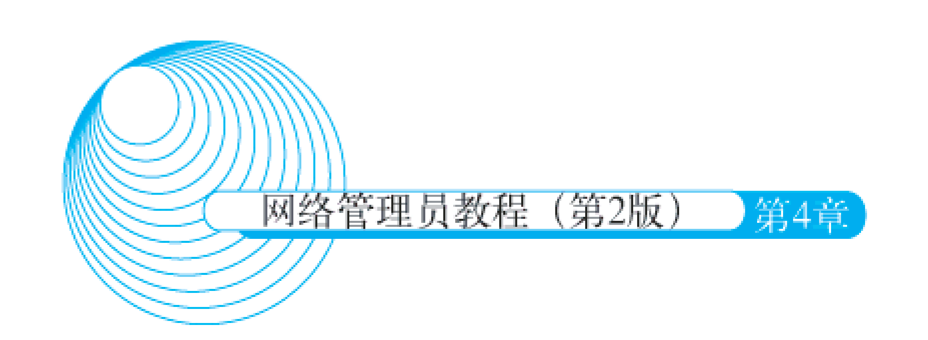
（4）具有安全性。网络操作系统的安全性主要体现在：具有严格的权限管理，用户通常分为系统管理员、高级用户和一般用户，不同级别的用户具有不同的权限；进入系统的每个用户都要审查，对用户的身份进行验证，执行某一特权操作也要进行审查；文件系统采取了相应的保护措施，不同程序有不同的运行方式。

4.1.2 网络操作系统的结构

当前在局域网（LAN）上配置的网络操作系统，基本上都是采用客户/服务器模式，因此，在客户/服务器模式的网络操作系统就由两部分组成：客户机（也称工作站）操作系统和服务器操作系统。

1. 工作站操作系统

工作站上配置操作系统的目的是：一方面工作站上的用户，可使用本地资源并执行在本地可以处理的应用程序和用户命令；另一方面实现工作站上的进程与服务器之间的交互。根据以



上两点，工作站操作系统可由单机操作系统直接扩充而成。要扩充的软件主要有：

（1）重定向程序（Redirector）。对于客户/服务器模式，工作站上的用户请求可分为本地请求和服务器请求，为使用户能以相同方式访问本地操作系统和远程服务器，在工作站应配置本地/远程请求解释程序。该程序在接收到工作站上用户发来的请求后，先判断该请求是本地请求还是服务器请求，如是本地请求则直接交给工作站操作系统进行处理；如是服务器请求，则按请求内容形成请求包，并通过传输软件，将其送给服务器。上面的本地/远程请求解释程序称为重定向程序。

（2）传输协议软件。为了实现工作站和服务器之间的通信，除了需要有网络硬件的支持外，还需要有网络协议的支持。目前在局域网上所采用的传输协议软件主要有 TCP/IP 协议软件和 SPX/IPX 协议软件。

2. 服务器操作系统

在客户/服务器模式下的网络系统主要指的就是服务器操作系统。位于网络服务器上的操作系统的主要功能包括：

（1）管理服务器上的各种资源，如处理机、存储器、I/O 设备以及数据库等；

（2）实现服务器与客户的通信；

（3）提供各种网络服务；

（4）提供网络安全管理。

为了实现上述功能，服务器操作系统应由以下软件组成：

（1）服务器操作系统的内核程序。为支持服务器中多进程的并发执行，要求服务器操作系统具有支持多进程（多任务）的功能；在此基础上应具有多用户文件管理、I/O 设备以及存储管理等功能，形成一个完整的操作系统。

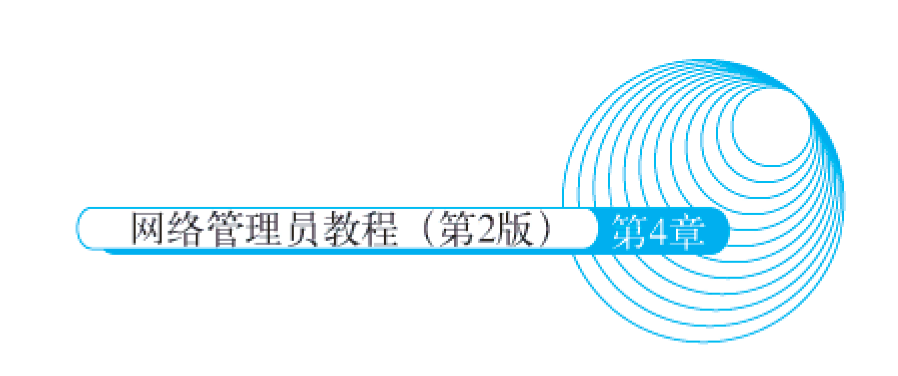
（2）传输协议软件。为支持服务器的客户之间传输信息，服务器操作系统也应提供传输协议软件。

（3）网络服务软件。为支持服务器上资源共享，网络服务器操作系统应提供一些核外实用程序供客户应用程序使用。这些网络服务软件可以是文件服务、打印服务、电子邮件服务等。

（4）网络安全管理软件。网络操作系统应对不同用户赋予不同的访问权限，通过规定对文件和目录的存取权限等措施，实现网络的安全管理。另外为了监测网络性能，及时了解网络运行情况和发现故障，网络操作系统应配置网络管理软件。

4.1.3 常见的网络操作系统

网络操作系统是组建网络的关键因素之一，目前流行的网络操作系统软件主要有 UNIX、Windows、Linux 和 NetWare 等。



1. UNIX 操作系统

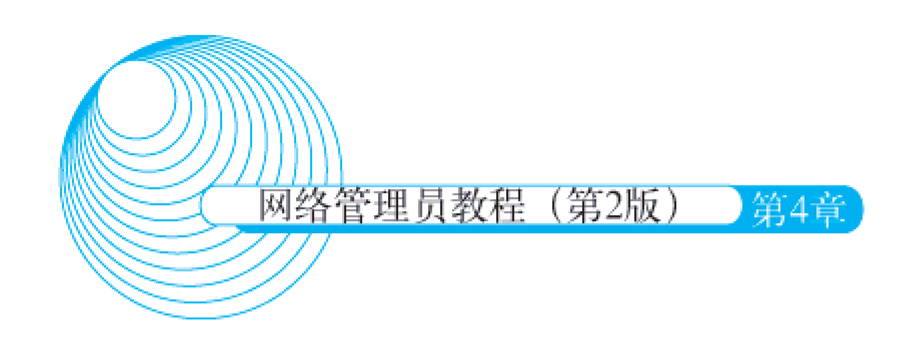
UNIX 系统是在美国麻省理工学院(MIT)1965 年开发的分时操作系统 Multics 的基础上不断演变而来的,它原是 MIT 和贝尔实验室等为美国国防部研制的。贝尔实验室的系统程序设计人员汤普逊(Thompson)和里奇(Ritchie)于 1969 年在 PDP—7 计算机上成功地开发了 16 位微机操作系统。该系统继承了 Multics 系统的树型结构、Shell 命令语言和面向过程的结构化设计方法,以及采用高级语言编写操作系统等特点,同时,又摈弃了它的许多不足之处。为了表示它与 Multics 既继承又扬弃的关系,该系统命名为 UNIX,UNIX 中的 UNI 正好与 Multi 相对照,表示 UNIX 系统不像 Multics 系统那样庞大和复杂,而 X 则是 cs 的谐音。

1972 年,UNIX 系统开始移植到 PDP-Ⅱ系列机上运行,1979 年,贝尔实验室又将其移植到类似于 IBM370 的 32 位机上运行,并公布了 UNIX 第 7 版。1980 年又公布了为 VAX-Ⅱ/780 计算机编写的操作系统 UNIX32V。在此基础上,加利福尼亚大学伯克利分校同年发表了 VAX-Ⅱ型机用的 BSD 4.0 和 BSD 4.1 版本。1982 年,贝尔实验室又相继公布了 UNIX System Ⅲ的 3.0、4.0 和 5.0 等版本。它们是对 UNIX32V 的改进,但却不同于 BSD 4.0 和 BSD 4.1 版本。1983 年 AT&T 推出了 UNIX Systems V 和几种微处理机上的 UNIX 操作系统。而伯克利分校公布了 BSD 4.2 版本。在 1986 年,UNIX Systems V 又发展为它的改进版 Res 2.1 和 Res 3.0,而 BSD 4.2 又升级为 BSD 4.3。

在这种背景下,IEEE 组织成立了 POSIX 委员会专门进行 UNIX 的标准化方面的工作。此外,在 1988 年以 AT&T 和 Sun Micro System 等公司为代表的 UI(UNIX International)和以 DEC、IBM 等公司为代表的 OSF(Open Software Foundation)组织也开始了这种标准化工作。它们与 UNIX 的开发工作虽然不一样,但它们定义出了 UNIX 的统一标准(可以运行 UNIX 应用软件的操作系统就是 UNIX)。从而统一 UNIX 系统的关键就变成是否能提供一个标准的用户界面,而不在于其系统内部是如何实现的了。

意识到 UNIX 系统的巨大价值,1980 年 8 月 Microsoft(1983 年从中分出 SCO)公司宣布它在 16 位(Intel 8086、Zelog 28000、Motorola M68000 等芯片)机上提供 UNIX 的微机版—Xenix,作为 UNIX 的商用系统。后来这一系统主要基于 Intel x86 芯片机器发展。Xenix 1.0 最早是基于 UNIX V7 开发的,后来又根据 UNIX System Ⅲ,UNIX System V 的各种版本作了裁剪、更新和扩充,形成了一系列版本 Xenix 1.x、Xenix 2.x 等。由于与 Microsoft 的关系,Xenix 上提供存取 MS-DOS 格式的文件及磁盘的命令。这种传统一直被 SCO 继承了下来,这也是之所以 Xenix 及后来的 SCO UNIX 在 PC 机上使用最为广泛的原因之一。

目前,UNIX 操作系统在商业领域逐步发展成为功能最强、安全性和稳定性最好的网络操作系统,但通常与服务器硬件产品集成在一起,较具有代表性的有 IBM 公司的 AIX UNIX、SUN 公司的 Solaris UNIX 和 HP 公司的 HP UNIX 等,各公司的 UNIX 比较适合运行于本公司的专



用服务器、工作站等设备上。

2．Windows 操作系统

Windows 起源可以追溯到 Xerox 公司进行的工作。1970 年，美国 Xerox 公司成立了著名的研究机构 Palo Alto Research Center(PARC)，从事局域网、激光打印机、图形用户接口和面向对象技术的研究，并于 1981 年宣布推出世界上第一个商用的 GUI(图形用户接口)系统—Star 8010 工作站。但如后来许多公司一样，由于种种原因，技术上的先进性并没有给它带来它所期望的商业上的成功。

当时，Apple Computer 公司的创始人之一 Steve Jobs，在参观 Xerox 公司的 PARC 研究中心后，认识到了图形用户接口的重要性以及广阔的市场前景，开始着手进行 GUI 系统研究开发工作，并于 1983 年研制成功第一个 GUI 系统——Apple Lisa。随后不久，Apple 又推出第二个 GUI 系统 Apple Macintosh，这是世界上第一个成功的商用 GUI 系统。当时，Apple 公司在开发 Macintosh 时，出于市场战略上的考虑，只开发了 Apple 公司自产微机上的 GUI 系统。而此时，基于 Intel x86 微处理器芯片的 IBM 兼容微机的出现，给 Microsoft 公司开发 Windows 提供了发展空间和市场。

Microsoft 公司 1983 年春季宣布开始研究开发 Windows。1985 年和 1987 年分别推出 Windows 1.03 版和 Windows 2.0 版。但是，由于当时硬件和 DOS 操作系统的限制，这两个版本并没有取得很大的成功。此后，Microsoft 公司对 Windows 的内存管理、图形界面做了重大改进，使图形界面更加美观并支持虚拟内存。Microsoft 于 1990 年 5 月份推出 Windows 3.0 并一举成功。

此后 Windows 操作系统产品出现了两条主线，一条是适合于桌面 PC 机运行的操作系统。如 1995 年推出的 Windows 95(又名 Chicago)，它可以独立运行而无需 DOS 支持。随后，陆续推出了 Windows 98、Windows ME、Windows 2000 Professional、Windows XP 等。另一条是网络操作系统 NT(New Technology)系列。

1993 年 6 月 Microsoft 公司发布了旨在与 UNIX 和 NetWare 竞争的 Windows NT 第一版 Windows NT 3.1，但由于存在很多缺陷，没有获得成功。1994 年 9 月，Microsoft 同时发布 Windows NT 3.5 和 BackOffice 应用包，Windows NT 3.5 的资源要求比 Windows NT 3.1 减少了 4MB，并增强了与 UNIX 和 NetWare 的连接和集成。1996 年 Microsoft 发布了 Windows NT 4.0 版，这种版本支持 Windows 95 界面，一种 Exchange 文电传送客户机和 Network OLE，后者允许软件对象经过网络进行通信。2000 年初融合了 Windows 98 和 Windows NT 的 Windows 2000(曾经命名为 Windows NT 5)问世。2003 年 4 月，恰逢“Windows NT 问世 10 周年”。Microsoft 发布了 Windows.NET Server 2003。

3. Linux 操作系统

1991 年，芬兰赫尔辛基大学的学生 Linus Torvalds 利用因特网，发布了他在 i386 个人计算机上开发的 Linux 操作系统内核的源代码，创建了具有全部 UNIX 特征的 Linux 操作系统。近年来，Linux 操作系统发展十分迅猛，每年的发展速度超过 200%，得到了包括 IBM、COMPAQ、HP、Oracle、Sybase、Informix 在内的许多著名软硬件公司的支持，目前 Linux 已全面进入应用领域。由于它是因特网和开放源码的基础，许多系统软件设计专家利用因特网共同对它进行了改进和提高。目前，直接形成了与 Windows 系列产品的竞争。究其原因，主要是 Linux 具有以下一些特点：

(1) 可完全免费得到。只要有快速的网络连接，Linux 操作系统可以从因特网上免费下载使用，而且，Linux 上跑的绝大多数应用程序也是免费可得的。

(2) 可以运行在 386 以上及各种 RISC 体系结构的机器上。Linux 最早诞生于微机环境，一系列版本都充分利用了 X86CPU 的任务切换能力，使 X86CPU 的效能发挥得淋漓尽致，而这一点 Windows 没有做到。此外，它可以很好地运行在由各种主流 RISC 芯片(ALPHA、MIPS、PowerPC、UltraSPARC、HP-PA 等)搭建的机器上。

(3) Linux 是 UNIX 的完整实现。Linux 是从一个成熟的 UNIX 操作系统发展而来的，UNIX 上的绝大多数命令都可以在 Linux 里找到并有所加强。UNIX 的可靠性、稳定性以及强大的网络功能也在 Linux 身上一一体现。

(4) 具有强大的网络功能。实际上，Linux 就是依靠因特网才迅速发展了起来，Linux 自然具有强大的网络功能。它可以轻松地与 TCP/IP、LAN Manager、Windows for Workgroups、Novell NetWare 或 Windows NT 网络集成在一起，还可以通过以太网或调制解调器连接到因特网上。Linux 不仅能够作为网络工作站使用，更可以胜任各类服务器的工作，如 X 应用服务器、文件服务器、打印服务器、邮件服务器、新闻服务器等。

(5) 是完整的 UNIX 开发平台。Linux 支持一系列的 UNIX 开发工具，几乎所有的主流程序设计语言都已移植到 Linux 上并可免费得到，如 C、C++、FORTRAN 77、ADA、PASCAL、Modual 2 和 Modual 3、Tcl/TkScheme、SmallTalk/X 等。

(6) 完全符合 POSIX 标准。POSIX 是基于 UNIX 的第一个操作系统簇国际标准，Linux 遵循这一标准使 UNIX 下许多应用程序可以很容易地移植到 Linux 下，相反也是这样。

4.2 Windows Server 2003 操作系统

4.2.1 Windows Server 2003 简介

Windows Server 2003 是继 Windows XP 后，Microsoft 发布的又一个最新产品，起初的名称

是 Windows. NET Server 2003，2003 年 1 月 9 日正式改名为 Windows Server 2003，名称虽然沿袭了 Windows 家族的习惯用法，但从其提供的各种内置服务以及重新设计的内核程序来说已经与 Windows 2000/XP 版有了本质的区别。此次升级 Microsoft 还添加了一个新的 Windows 2003 Web Edition 版，这个版本专门针对 Web 服务进行优化，并且与.NET 技术紧密结合，提供了快速的开发、部署 Web 服务和应用程序的平台。Windows Server 2003 家族成员如表 4-1 所示。

表 4-1　Windows Server 2003 家族成员

版本	硬件最大支持	服务特点
Windows Server 2003 Web Edition	2GB 内存、2 路处理器	针对 Web 服务进行优化。仅能够在 AD 域中做成员服务器，不能做 DC 域控制器
Windows Server 2003 Standard Edition	4GB 内存、4 路处理器	针对中小型企业。具备除元目录服务(MMS)支持、终端服务会话目录、集群服务以外的所有服务功能
Windows Server 2003 Enterprise Edition	64GB 内存、8 路处理器	针对高端服务的需求。具备所有服务功能
Windows Server 2003 Datacenter Edition	512GB 内存、32 路处理器	符合最高性能的要求，具有极其可靠的稳定性与扩展性。具备除 Internet 连接防火墙、Internet 连接共享以外的所有服务功能

1. Windows Server 2003 的主要功能

Windows Server 2003 是一个多任务操作系统，能够以集中或分布的方式实现各种应用服务器角色。这些应用服务器包括：

(1) 文件和打印服务器；

(2) Web 服务器和 Web 应用程序服务器；

(3) 邮件服务器；

(4) 终端服务器；

(5) 远程访问/虚拟专用网络(VPN)服务器；

(6) 目录服务器、域名系统(DNS)、动态主机配置(DHCP)服务器和 Windows 因特网命名服务器(WINS)；

(7) 流媒体服务器。

2．Windows Server 2003 的主要特点

（1）可靠性。Windows Server 2003 通过可靠、实用和灵活的集成结构，帮助用户确保商业信息的安全可靠。

（2）高效性。Windows Server 2003 的高效性主要体现在：通过提供灵活易用的工具，帮助用户设计、部署与组织网络；通过加强策略、使任务自动化以及简化升级来帮助用户主动管理网络；通过让用户自行处理更多的任务来降低支持开销。

（3）实用性。Windows Server 2003 提供集成的 Web 服务器和流媒体服务器，帮助用户快速、轻松和安全地创建动态 Intranet 和 Internet 的 Web 站点；提供集成的应用程序服务器，帮助用户轻松地开发、部署和管理 XML Web 服务；提供多种工具，使用户得以将 XML Web 服务与内部应用程序、供应商和合作伙伴连接起来。

（4）经济性。Windows Server 2003 能够紧密地与 Microsoft 及其合作伙伴的硬件、软件和服务相结合，帮助用户合并各个服务器，从而更好地优化服务器部署策略，降低用户的所属权总成本（TCO）。

3．Windows Server 2003 的新增功能

Windows Server 2003 在 Windows 2000 Server 的基础上增加了许多新功能，包括配置流程向导、远程桌面连接（TS）、Internet 信息服务（IIS 6.0）、简单的邮件服务器（POP3）、WMS（Windows Media Services）流式媒体服务器等。

（1）配置流程向导。Windows Server 2003 最大的特点是提供了多种多样的特色服务。有从 Windows 2000 版继承发展而来的“域控制（AD）服务”、“终端服务”、“IIS 服务”、“DNS 服务”等，还有新增加的“邮件服务”、“文件服务”等。由于服务的增多，给服务的配置带来了很多问题，在 Windows 2000 中经常为了配置一项服务而不得不打开多个界面，进行多个操作步骤，同时还需要用户具有一定的经验才可以完成。这项工作被 Windows Server 2003 中的一个统一的配置流程向导，即“管理您的服务器”所替代，如图 4-1 所示。

（2）终端服务器—远程桌面连接（TS）。在 Windows 2000 中若要使用“远程桌面连接”就必须打开一个独立的窗口，以便在这个窗口中操作远程主机。这种操作方式对于少量的连接还可以承受，然而对于那些要进行大量的连接以及在各连接窗口间进行的频繁操作来说，这种方式往往会产生数据混乱、操作对象不清等严重的后果。Windows Server 2003 对于“远程桌面连接”的操作方式进行了大幅的调整，从以前单一的连接窗口改为了树状控制台与连接显示窗口相结合的统一管理平台，如图 4-2 所示。任何的连接与切换都可以在这个平台内进行操作与管理。同时，用户可以随意自定义连接屏幕的尺寸大小，以适应不同的显示要求。

（3）Internet 信息服务 6.0（IIS 6.0）。IIS 6.0 在以下几个方面进行了改进：

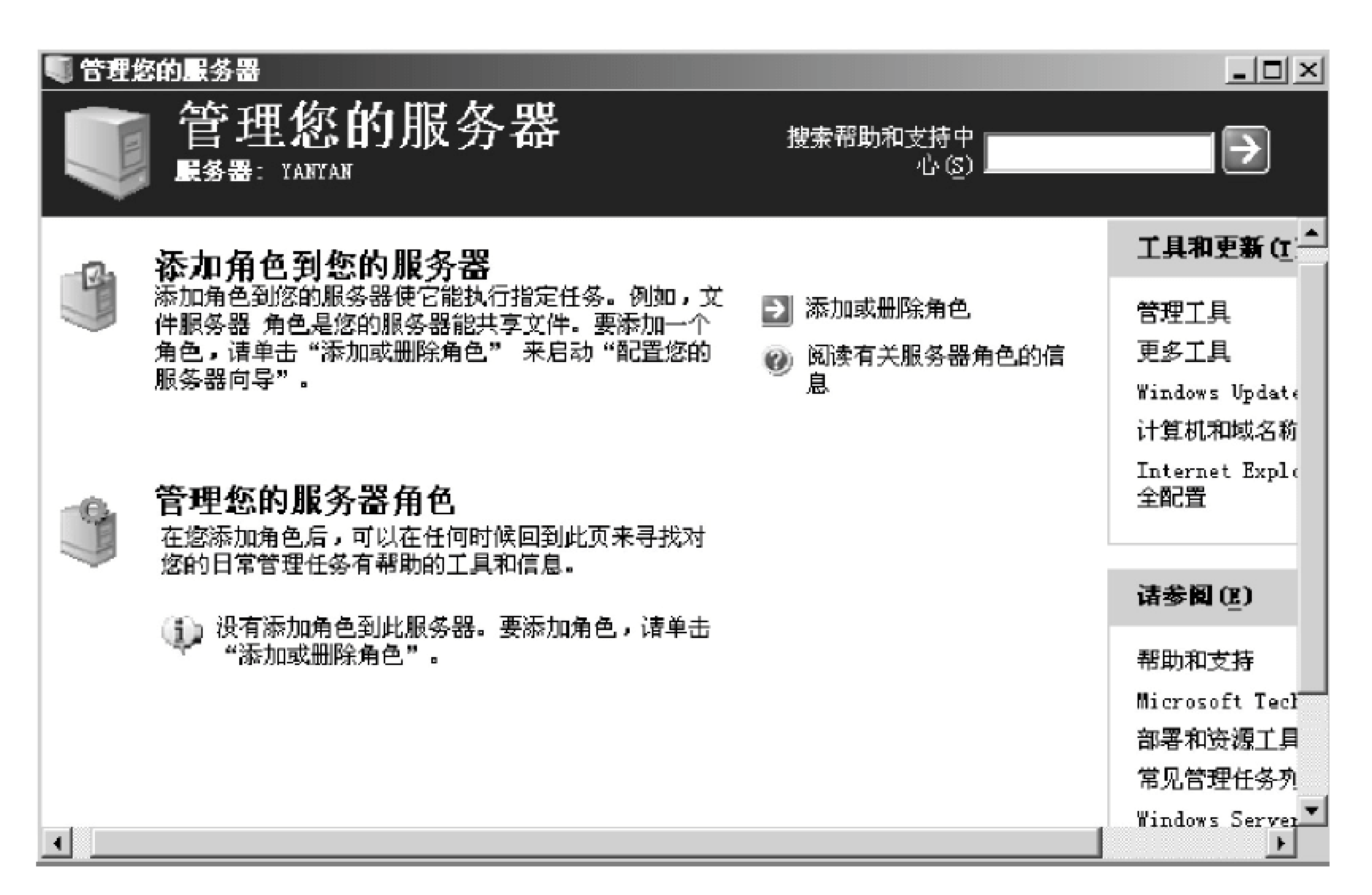


图 4-1 “管理您的服务器”界面



图 4-2 “远程桌面”连接界面

① 增强了可靠性。整合了.NET 服务，所有的页面以及交互动作都可以在预编译的情况下进行处理，对于内存的泄漏、非法访问及其他错误，IIS 6.0 都会自动探测，并在底层进行容错与

排除。

② 增强了方便性。管理员可以根据需要方便地对各种 Web 服务组件进行添加、禁止、授权等操作。例如若要添加一个新的 Web 服务，只须单击“添加一个新 Web 服务扩展”的链接，在弹出的窗口中指定扩展名和所需的扩展文件，这个 Web 服务就自动添加到了系统中了，一切操作都非常便捷。

③ 增强了安全性。当服务器发生严重故障时，XML-Metabase 可以提供有效的备份与恢复手段，可以使用任何一种 XML 编辑器在线编辑它并且立即生效，且无须重新启动服务器。另外，还增加了多种加密及安全运行的手段，有传统的 SSL、CA 证书，还有新增的 passport、通用语言进行时（CLR，Common Language Runtime）。

④ 增强了扩展性。IIS6 与 ASP. NET 的无缝整合，以及多达十几种的开发语言的选择，给开发者提供了一个快速应用程序开发（RAD）平台。

⑤ 增强了兼容性。IIS6 兼容 Unicode 架构的 HTTP 协议，可以使客户利用 Unicode 格式访问服务器变量，同时也允许开发者访问 URL 的 Unicode 表达式。

需要指出的是，IIS 6.0 在默认情况下并不会被安装在 Windows Server 2003 上，这需要管理员手动进行安装。IIS 6.0 服务器界面如图 4-3 所示。

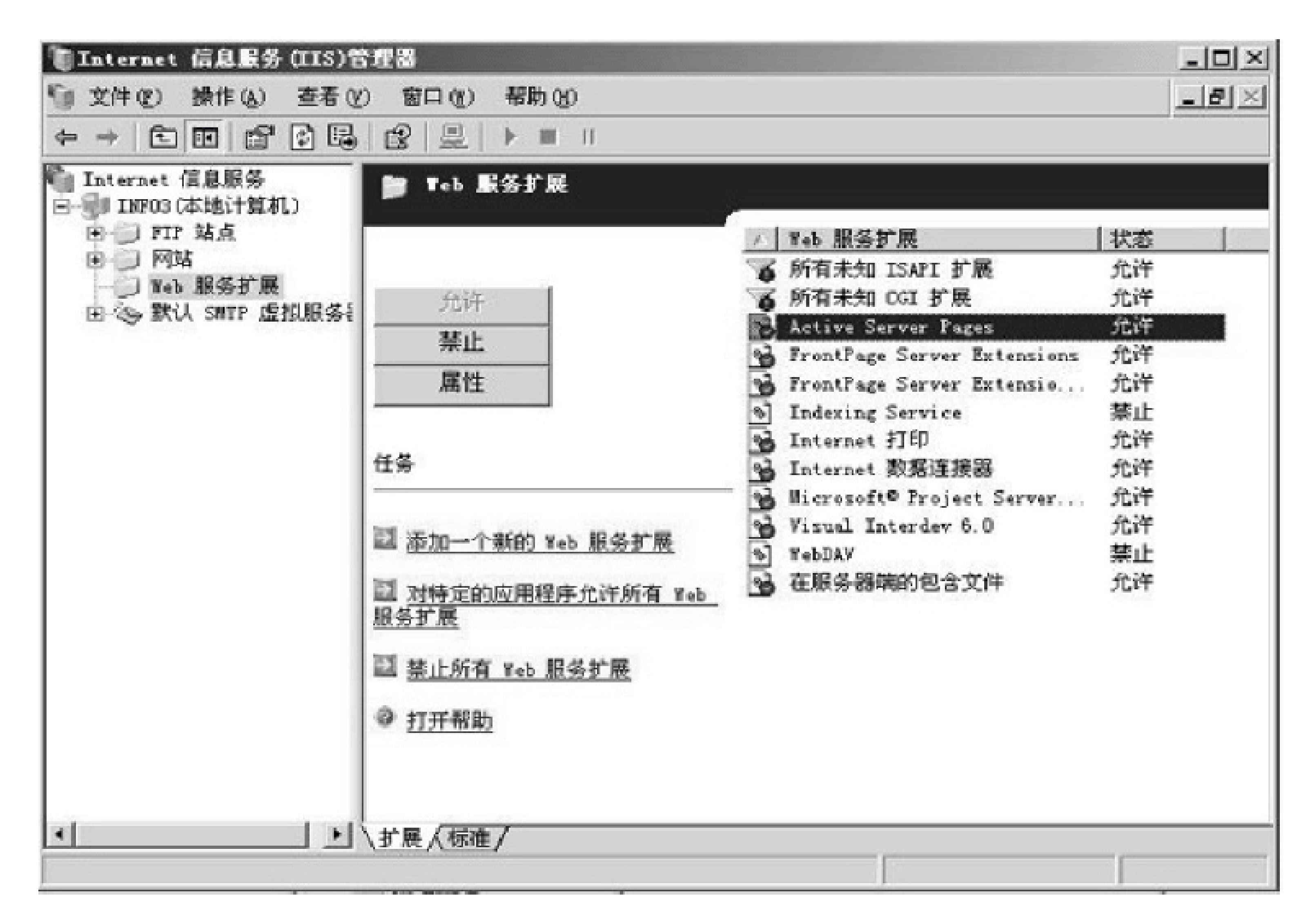


图 4-3　IIS 6.0 服务器界面

（4）简单的邮件服务器（POP3）。邮件服务器（POP3）是 Windows Server 2003 新增的功能，它的配置非常的简单，只需几个步骤就可以完成，简单邮件服务器界面如图 4-4 所示。但与专业的邮件服务器相比它只能算是一个具备收发邮件功能的简单服务器，尚未涉及到容量控制、邮

件转发、用户信息维护等功能。

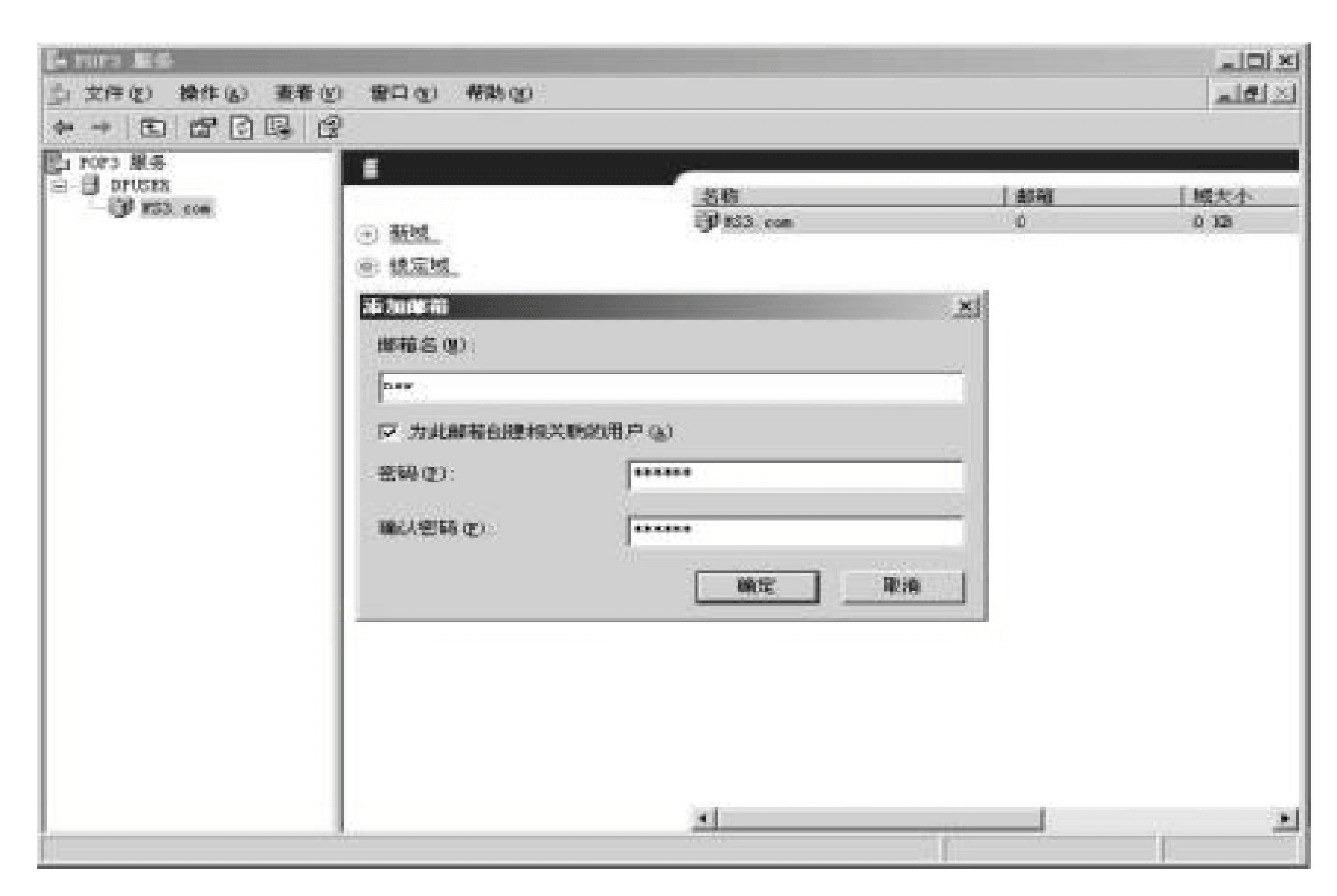


图 4-4　POP3 服务配置窗口

（5）流式媒体服务器（WMS，Windows Media Services）。WMS 是 Windows 多媒体技术用于在 Internet 与 Intranet 分发数字媒体内容的服务器端组件。它在 Windows 2000 中已经出现了，在 Windows 2003 中除了版本已经升到 9.0 以外，其内部的各项服务也已经被重新设计和增强，如图 4-5 所示。

WMS9 在电影点播、电台播放、视频会议、远程教育/培训等方面的应用具备先天的优势。此次被 Windows Server 2003 作为一项服务整合在其中，在功能、管理、成本等多方面得到进一步的升华。主要表现在：

① 支持快速的媒体流。WMS9 解决了媒体播放的缓存延迟问题。另外在信号发生中断的情况下，WMS 服务器会自动恢复播放器与服务器、服务器与服务器之间的数据连接，避免了因信号的突然中断而导致的连接丢失。

② WMS9 可以像普通的电视台一样连续的播放节目，只须在服务器端添加播放列表（相当于电视台的节目单）来安排当日的所有播放内容。并且提供了在播放的同时动态更改播放内容而无须中断观看的功能。

③ WMS9 系统支持多种广告类型的播放，包括节目前的广告和插播广告等，只需简单的配置就可轻松实现。同时，它还可以集成第三方的广告服务器。

④ 管理者可以通过 MMC（Microsoft 管理控制台）、Web 浏览器、命令行脚本这三种方式在任何的环境下实现对 WMS9 服务器的管理，其中 Web 浏览器可以通过 SSL 加密处理来进行安

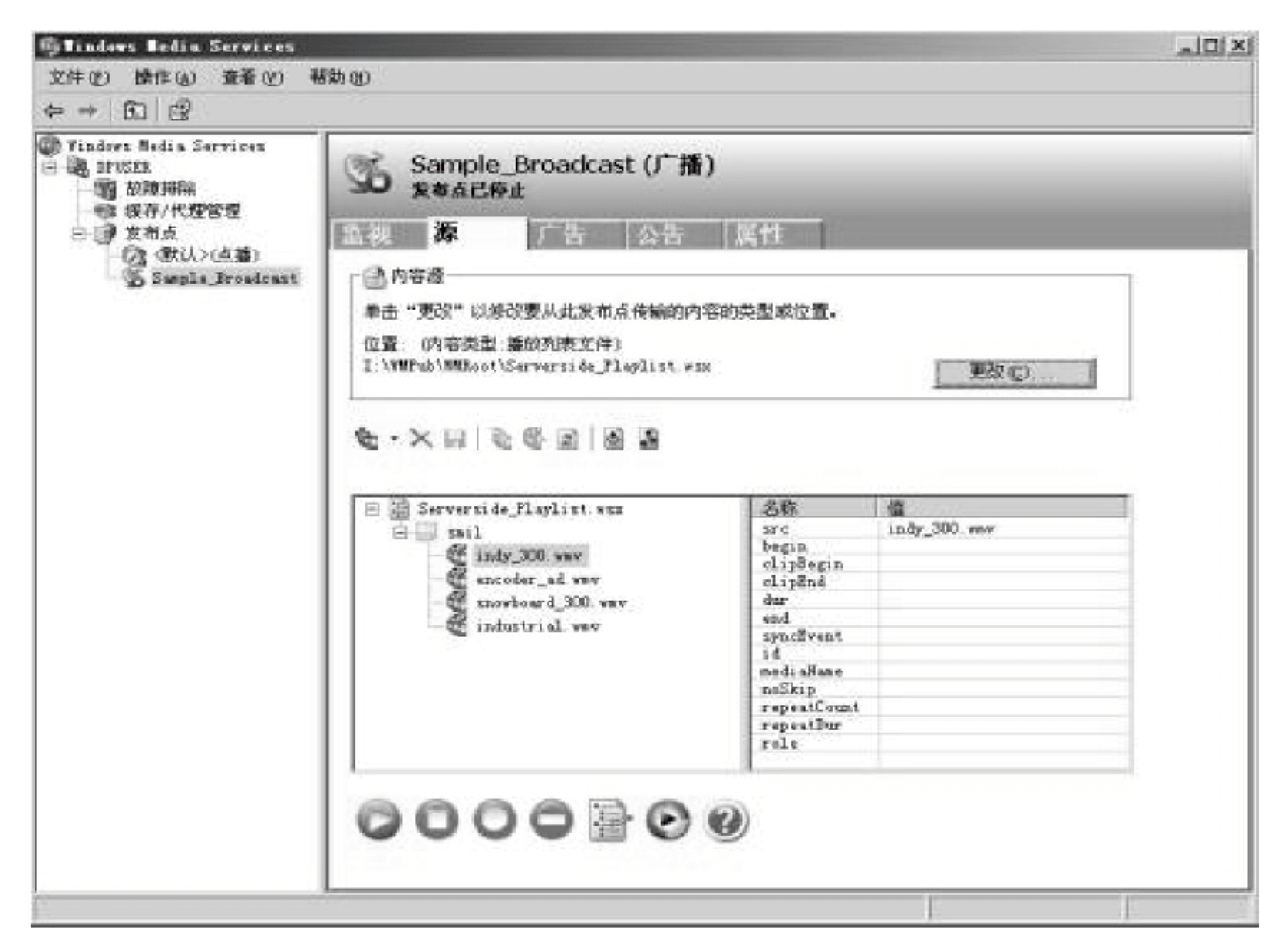


图 4-5　流式媒体服务器操作界面

全的连接。

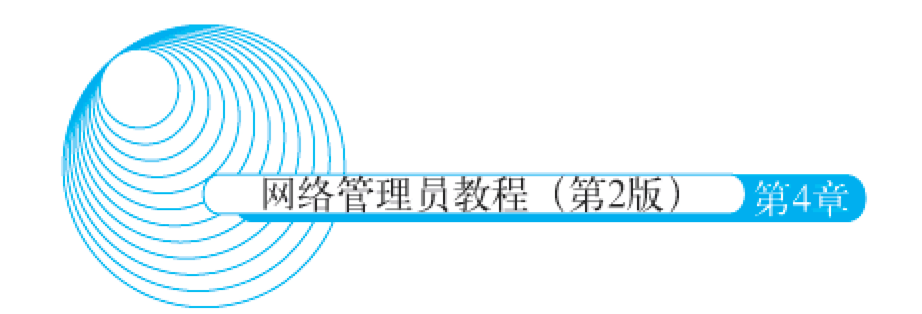
⑤ WMS 提供了超过 700 个业内标准的服务器接口，开发人员可以通过使用.NET 支持的各种语言，以非常容易的手段来扩展/定制媒体服务的各种功能。

(6) 系统关闭事件跟踪。如果用户不得不关闭或重启系统，Windows Server 2003 需要用户提供关闭计算机的原因（硬件维护、应用程序安装、安全问题等），并附加一些说明注释，才允许关闭系统。这样，不仅可以保证用户的任何操作在系统的监视记录之下进行，而且还可以为以后的维护管理提供可以遵循的标准化信息。

4.2.2　Windows Server 2003 的安装

Windows Server 2003 家族包括 Windows Server 2003 标准版、Windows Server 2003 企业版、Windows Server 2003 数据中心版、Windows Server 2003 Web 版等产品，安装时用户可以选择。安装时系统的硬件环境建议 CPU 主频在 733MHz 以上，内存 256MB 以上，硬盘 2GB 以上，监视器的分辨率 800×600 以上。

Windows Server 2003 的安装继承了 Windows 产品安装时方便、快捷、高效的特点，几乎不需要多少人工参与就可以自动完成硬件的检测、安装、配置等工作，需要做的仅是通过屏幕来了



解它所提供的各项新技术以及产品特点。安装过程中会收集区域信息、语言信息、个人注册信息、产品序列号、计算机/管理员基本信息、网络基本信息等。Windows Server 2003 的安装过程如下：

（1）在启动计算机的时候进入 CMOS 设置，把系统启动选项改为光盘启动，保存配置后放入系统光盘，重新启动计算机，让计算机用系统光盘启动。启动后，系统读取启动文件，首先出现的画面是硬件选择，例如有没有 SCSI、RAID 等。接下来开始向计算机复制安装所需要的文件及驱动程序，接着询问用户是否安装此操作系统，按 Enter 键确定安装，按 R 键进行修复，按 F3 键退出安装，如图 4-6 所示。

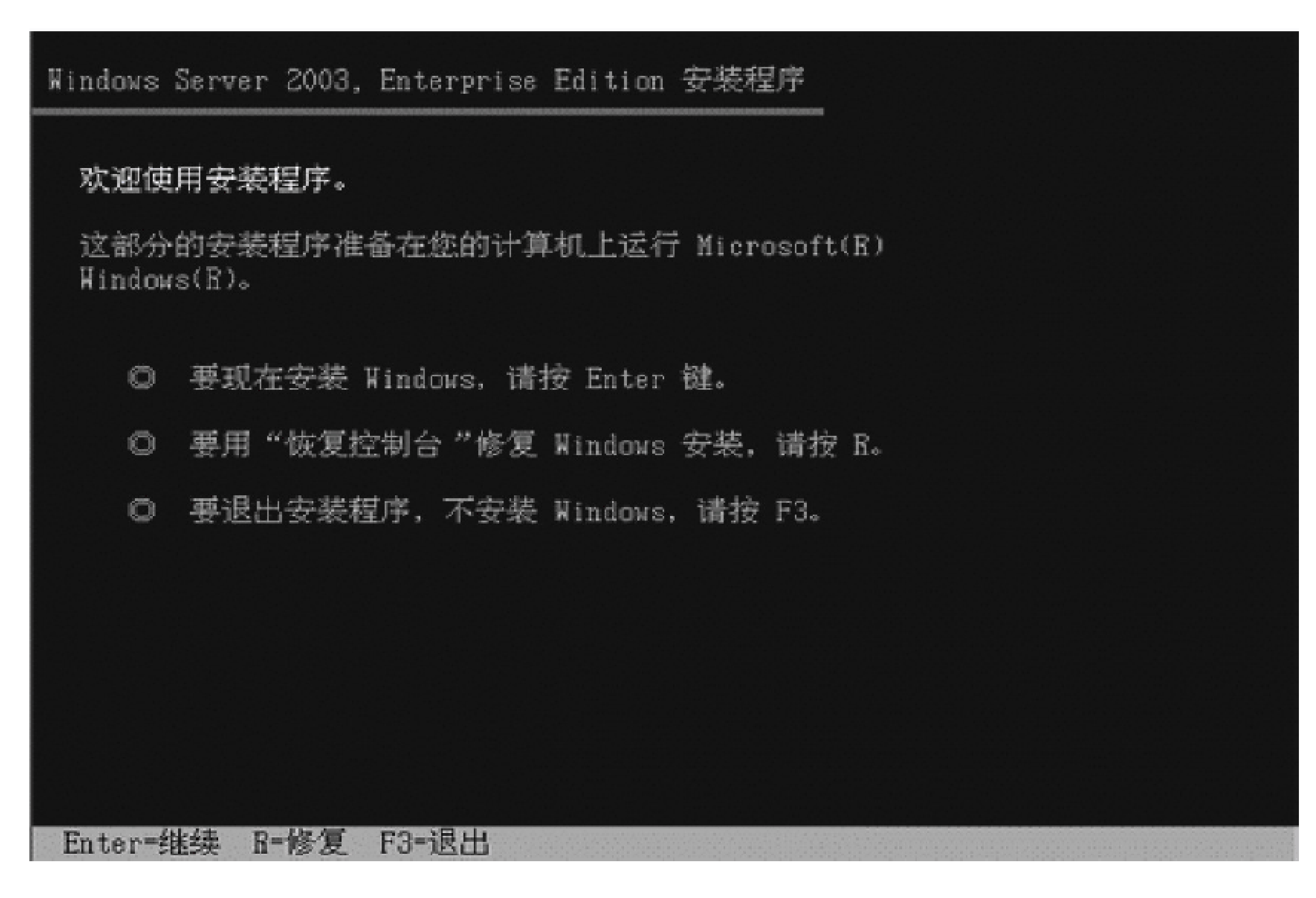


图 4-6　Windows Server 2003 安装程序初始界面

（2）按 Enter 键确认安装，接下来出现软件的授权协议，必须按 F8 键同意其协议方能继续进行，下面将搜索系统中已安装的操作系统，并询问用户将操作系统安装到系统的哪个分区中，如果是第一次安装系统，需要用光标键选定需要安装的分区，如图 4-7 所示。

（3）选定分区后，系统会询问用户把分区格式化成哪种分区格式，建议格式化为 NTFS 格式；对于已经格式化的磁盘，软件会询问用户是保持现有的分区还是重新将分区修改为 NTFS 或 FAT 格式的分区，同样建议修改为 NTFS 格式分区。选定后按 Enter 键，系统将从光盘复制安装文件到硬盘上。当安装文件复制完毕后，第一次重新启动计算机。

NTFS 是随着 Windows NT 操作系统而产生的，并随着 Windows NT 4 跨入主力分区格式的行列，它的优点是安全性和稳定性极其出色。Windows 2000、Windows XP 和 Windows Server

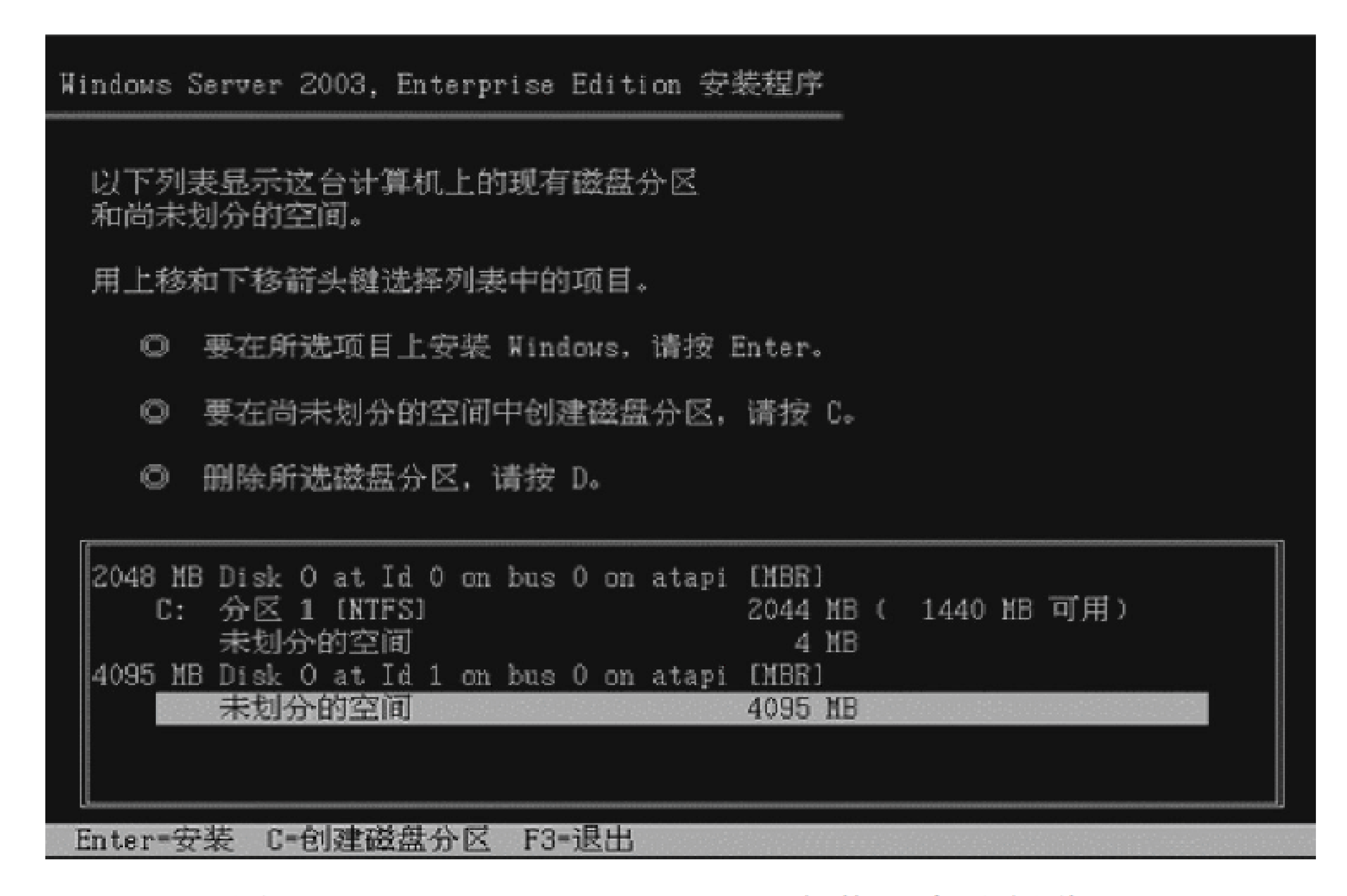


图 4-7　Windows Server 2003 安装程序选择分区

2003 都是基于 Windows NT 的技术，提供对完善的 NTFS 分区格式的支持。NTFS 文件系统的安全性，主要的作用体现在以下几个方面：

① NTFS 分区对用户权限作出了非常严格的限制，每个用户都只能按照系统赋予的权限进行操作，任何试图越权的操作都将被系统禁止。在一个格式化为 NTFS 的分区上，每个文件或者文件夹都可以单独的分配一个许可，这个许可使得这些资源具备更高级别的安全性，用户无论是在本机还是通过远程网络访问设有 NTFS 许可的资源，都必须具备访问这些资源的权限。

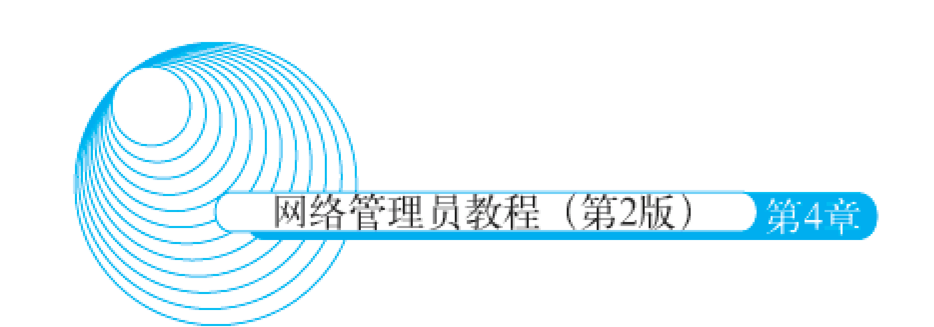
② NTFS 支持对单个文件或者目录的压缩。这种压缩不同于 FAT 结构中，对驱动器卷的压缩，其可控性和速度都要比 FAT 的磁盘压缩要好的多。

③ NTFS 使用事务日志自动记录所有文件夹和文件更新，当出现系统损坏和电源故障等问题而引起操作失败后，系统能够利用日志文件重做或恢复未成功的操作，从而保护了系统的安全。

除了以上 3 个主要的特点之外，NTFS 文件系统还具有其他的优点，如：对于超过 4GB 以上的硬盘，使用 NTFS 分区，可以减少磁盘碎片的数量，大大提高硬盘的利用率；NTFS 可以支持的文件大小可以达到 64GB，远远大于 FAT32 下的 4GB；支持长文件名；等等。

(4) 系统重新启动后，即进入如图 4-8 所示的窗口界面，开始正式安装。在安装过程中，由于系统要检测硬件设备，屏幕可能会出现抖动，这是正常的。

(5) 在安装过程中，有几步需要用户参与如系统语言选择、用户信息的配置等，如图 4-9 所示，一般说来，只要使用默认设置即可，直接单击“下一步”按钮。



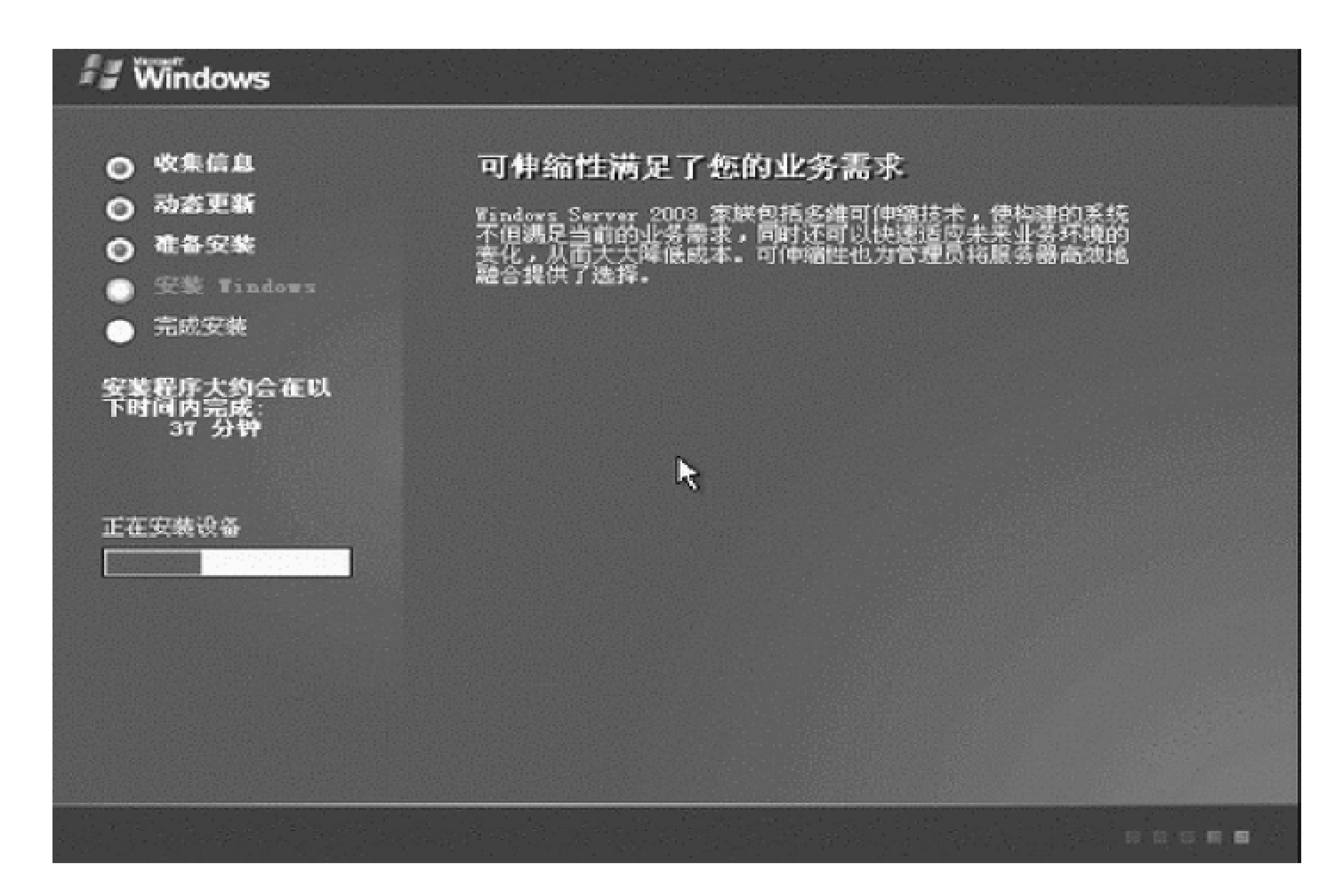


图 4-8　Windows Server 2003 安装程序开始界面

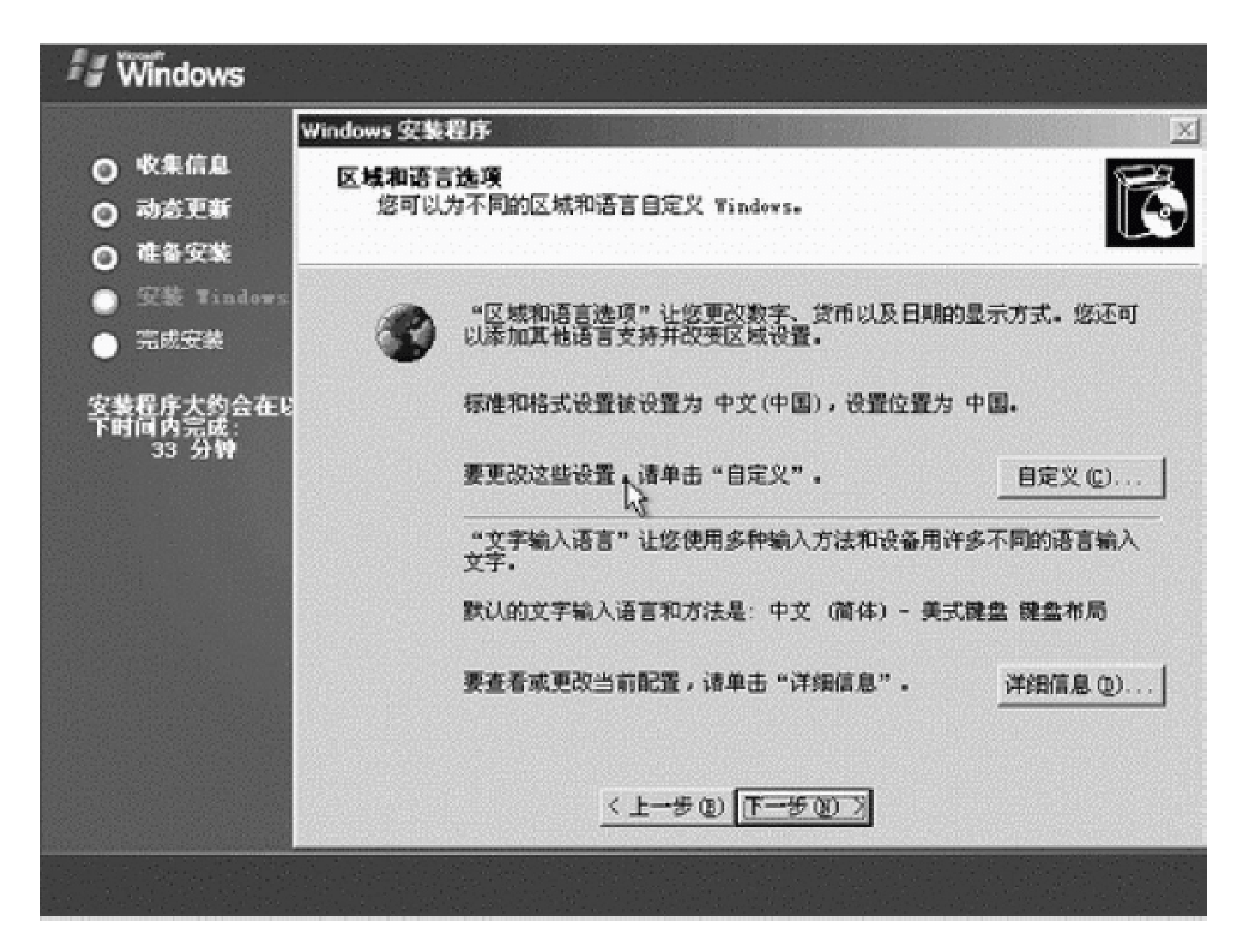


图 4-9　Windows Server 2003 安装程序语言选择

(6) 输入软件的序列号，在光盘盒或者说明书中找到序列号，输入到如图 4-10 所示的“产品密钥”文本框中，单击“下一步”按钮。

(7) 设置此服务器提供多少客户端连接，如图 4-11 所示，此时需要参考说明书的授权和局域网的实际情况，输入客户端数量。设置完毕后，单击“下一步”按钮。

(8) 设置计算机的名称和本机系统管理员的密码，如图 4-12 所示，计算机的名称不能与局

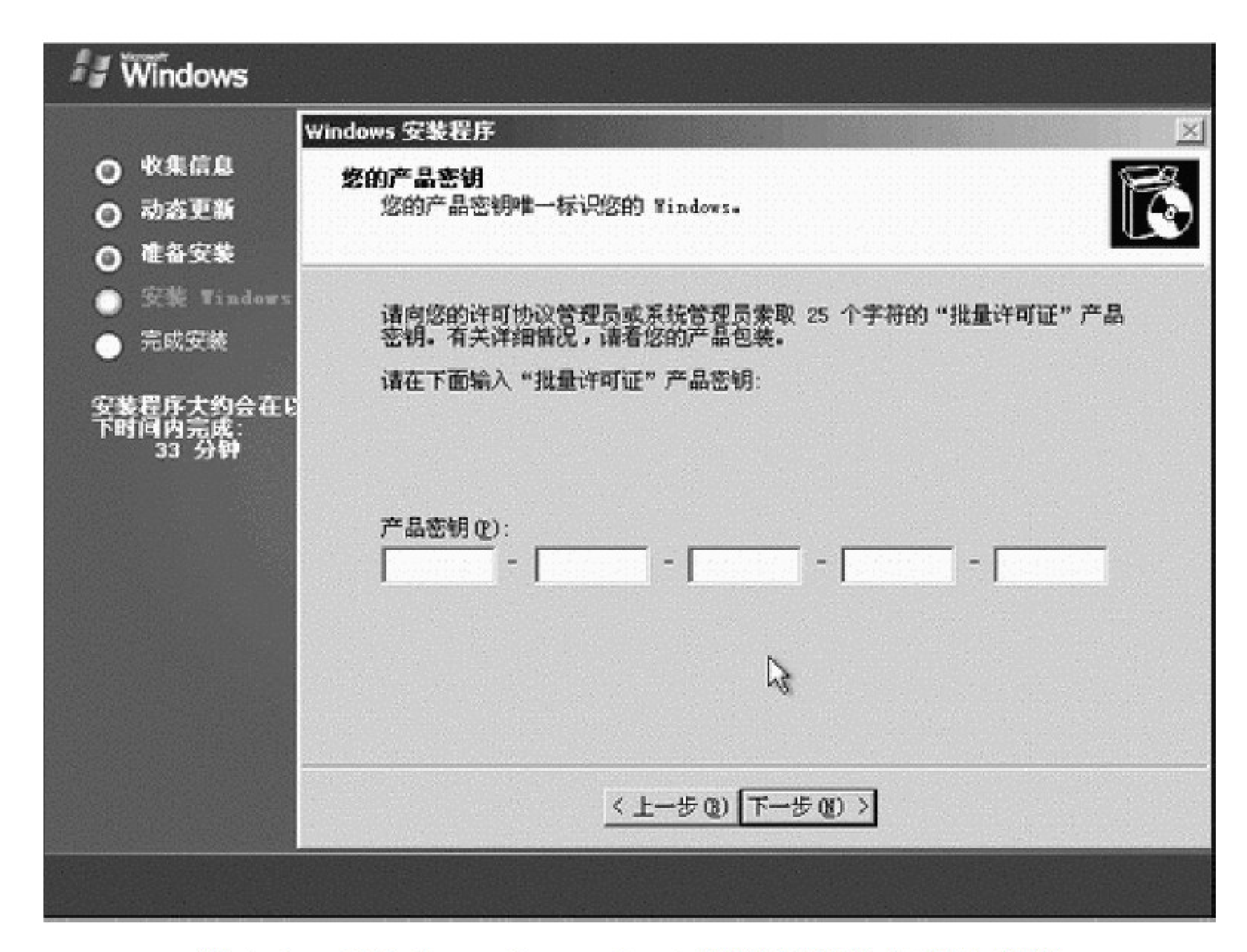


图 4-10　Windows Server 2003 安装程序输入产品密钥

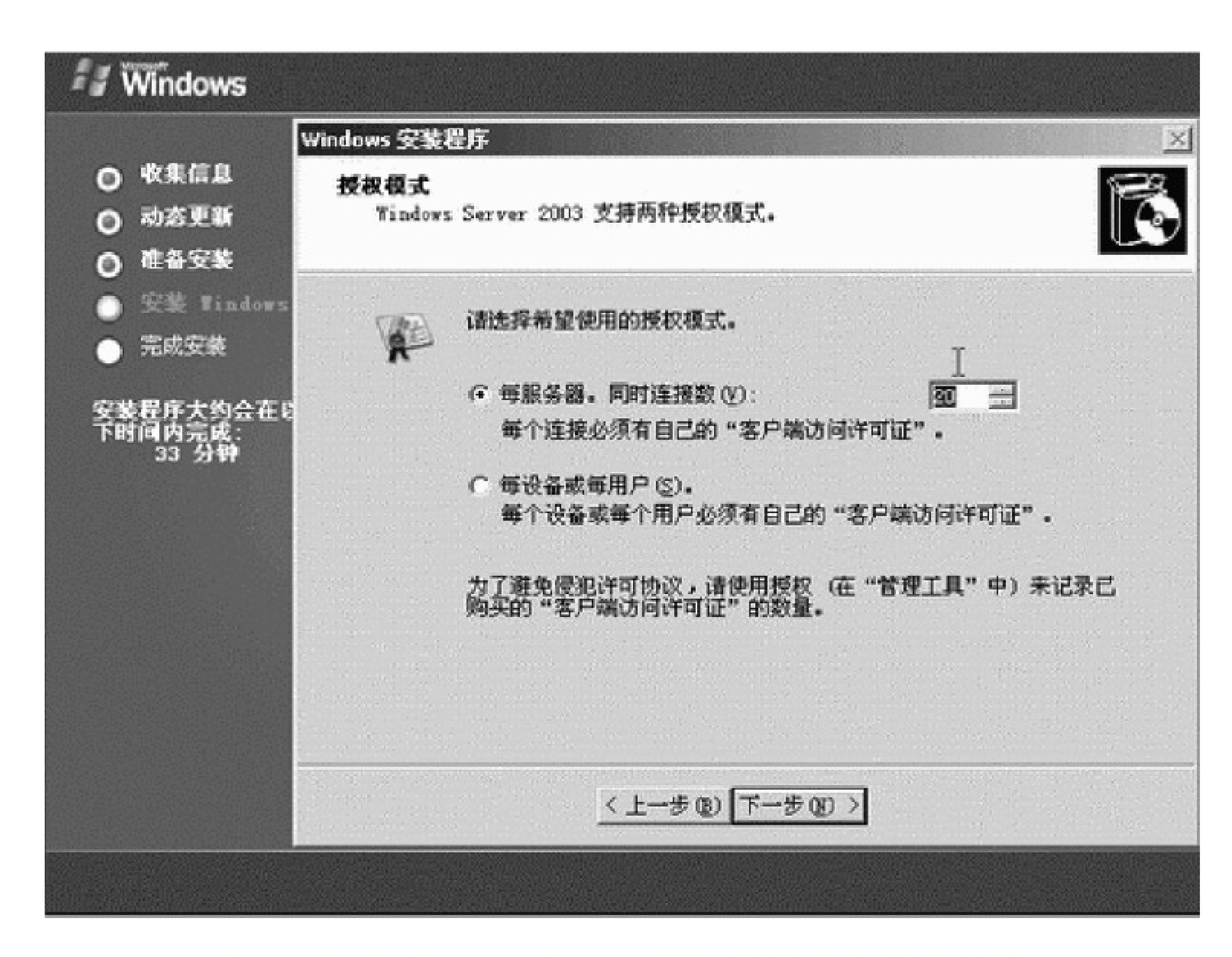
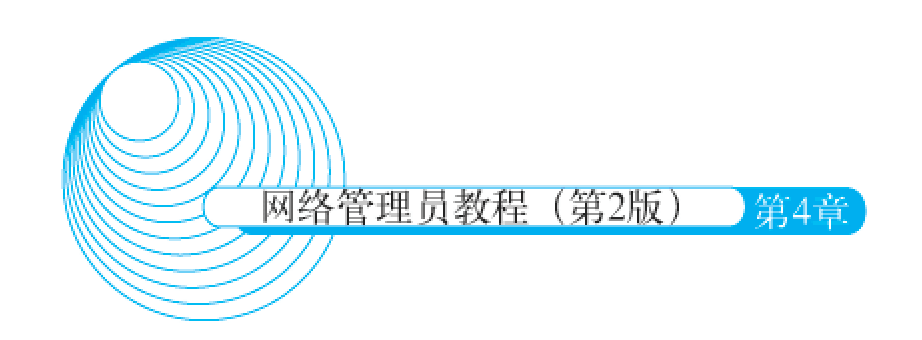


图 4-11　Windows Server 2003 安装程序授权界面

域网内其他计算机的名称相同，管理员的密码设置要安全，最好是数字、大写字母、小写字母、特



殊字符相结合，然后单击“下一步”按钮。



图 4-12　Windows Server 2003 安装程序输入管理员密码

(9) 设置网络，在这里可以选择“典型设置”，在安装完毕后再进行调整，如图 4-13 所示。

(10) 设置工作组或计算机域，不论是单机还是局域网服务器，最好是选中第一项，当把系统安装完毕后再进行详细的设置，如图 4-14 所示。

(11) 设置完毕后，系统将安装开始菜单项、对组件进行注册等进行最后的设置，这些都无需用户参与，所有的设置完毕并保存后，系统进行第二次启动。第二次启动，需要按 Ctrl＋Alt＋Del 组合键，然后输入管理员的密码登录系统，如图 4-15 所示。进入系统之后，将自动弹出一个“管理您的服务器”窗口，如前面图 4-1 所示。用户可根据需要进行详细配置，也可以后配置。

4.2.3　Windows Server 2003 的配置

1. 修改计算机名

通常在计算机安装完毕后都需要进行计算机名的修改。具体的操作步骤为：

(1) 通过菜单“开始”→“控制面板”→“系统”打开配置窗口，单击“计算机名”标签，如图 4-16 所示。

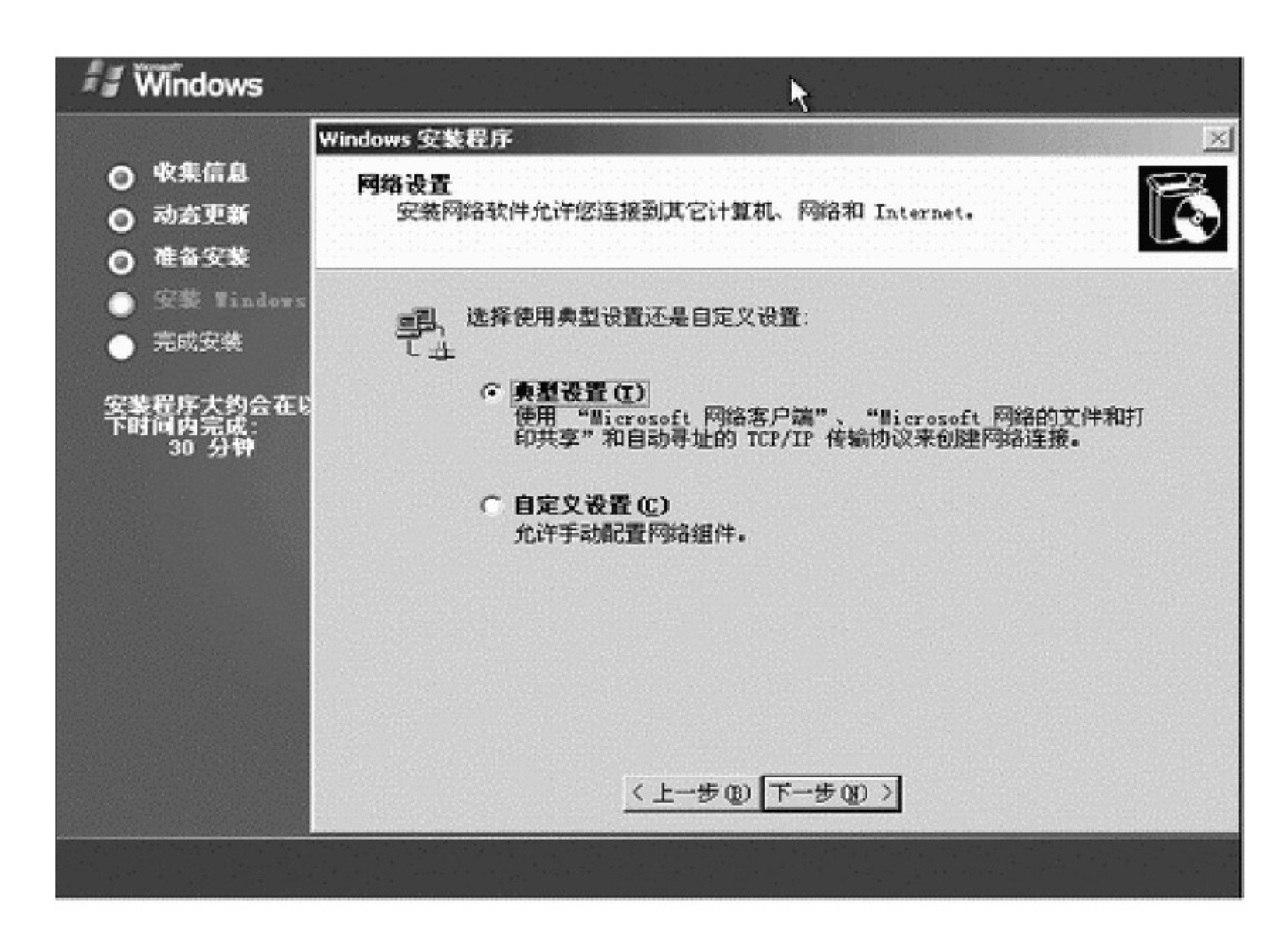


图 4-13　Windows Server 2003 安装程序网络设置

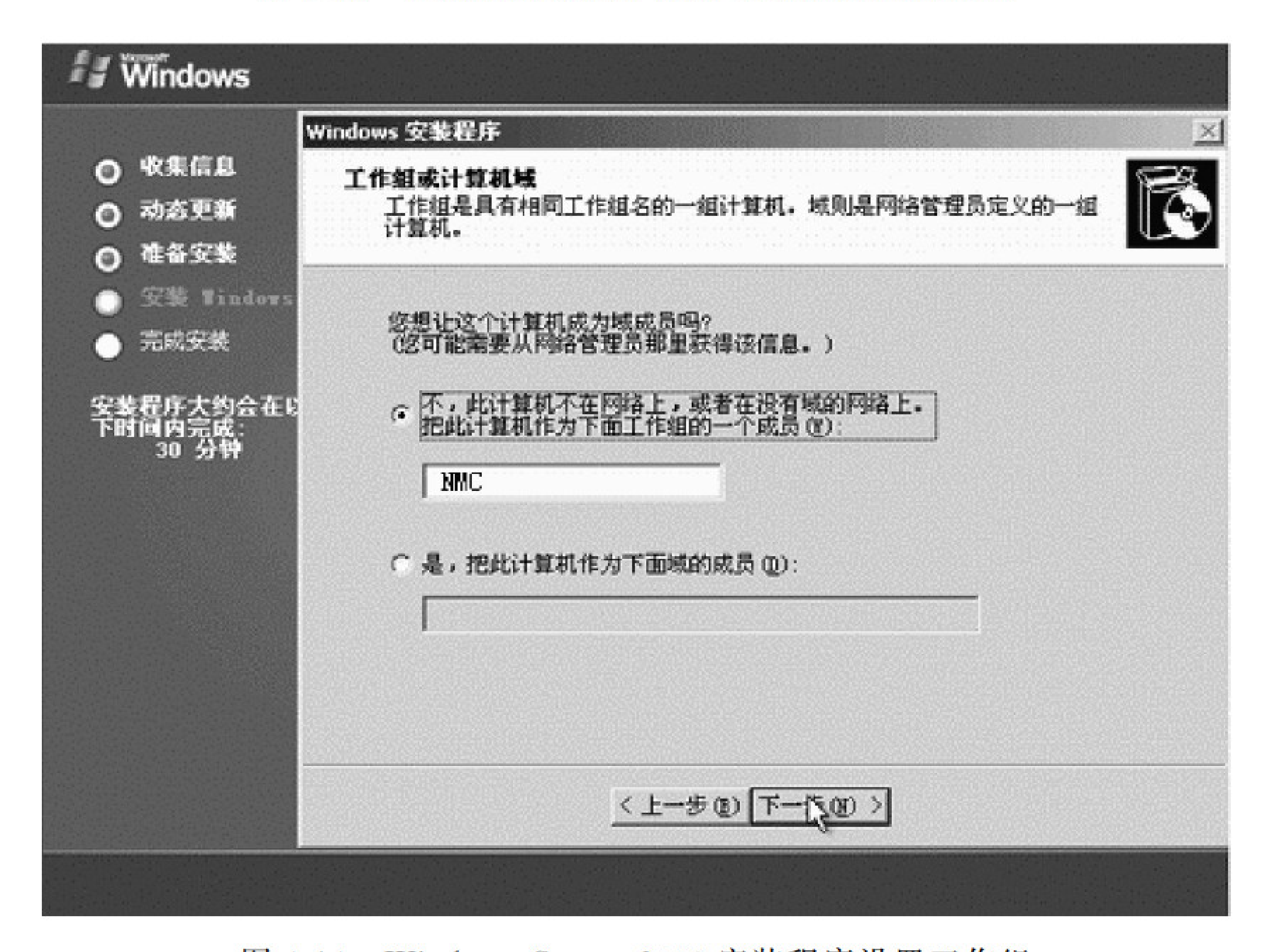
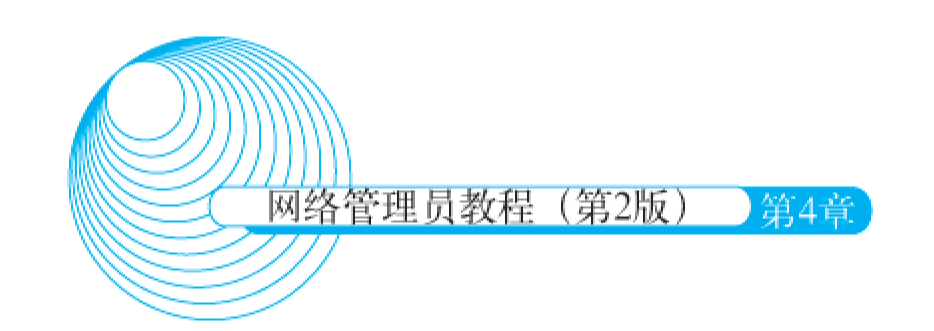


图 4-14　Windows Server 2003 安装程序设置工作组



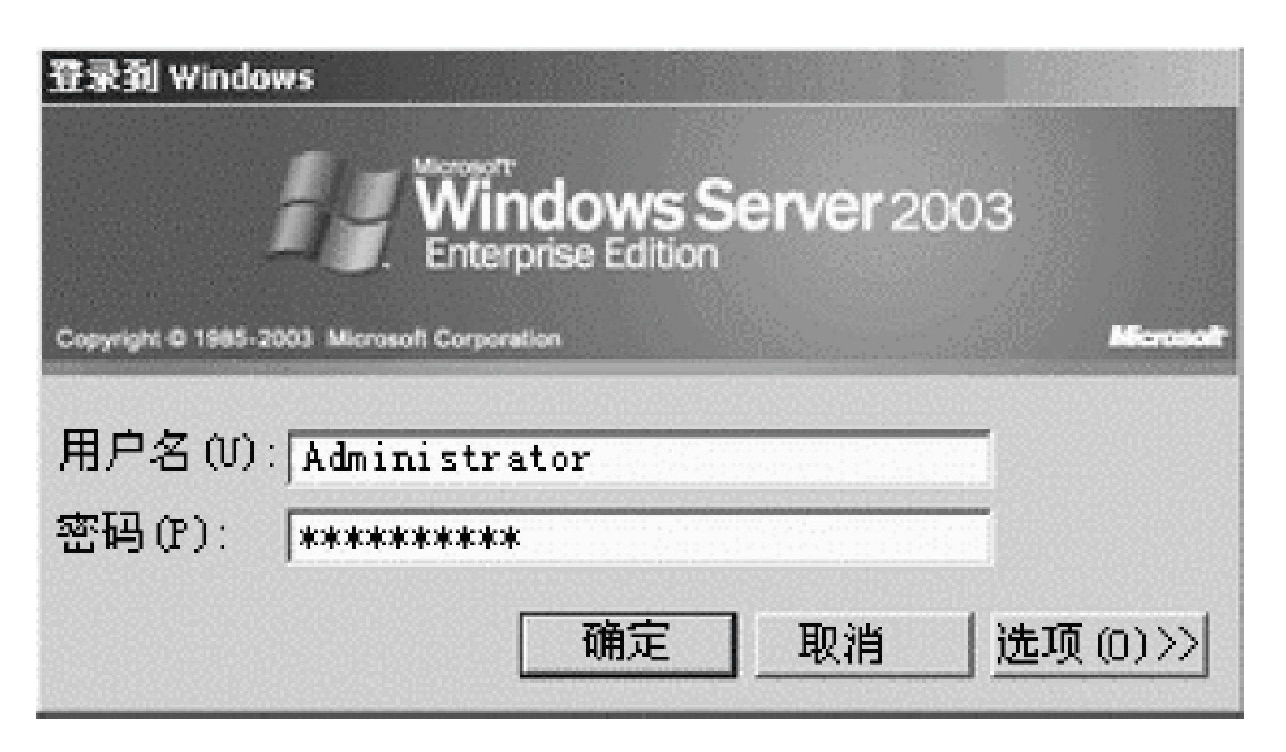


图 4-15 Windows Server 2003 登录界面

(2) 单击“更改”按钮，输入计算机名，然后在下方选择这台计算机是隶属于域还是工作组，如图 4-17 所示，单击“确定”按钮。



图 4-16 系统属性对话框



图 4-17 修改计算机名称对话框

2. 本地用户与组

为了保障计算机与网络的安全，Windows Server 2003 为不同的用户设置不同的权限，同时通过将具有同一权限的用户设置为一个组来简化对用户的管理。使用“本地用户和组”可创建并管理存储在本地计算机上的用户和组。添加用户的步骤为：

(1) 依次单击“开始”→“管理工具”→“计算机管理”，将显示“计算机管理”窗口，如图 4-18 所示。

(2) 双击“本地用户和组”，在右侧的“名称”窗口中将出现“用户”和“组”两个目录，目录内分

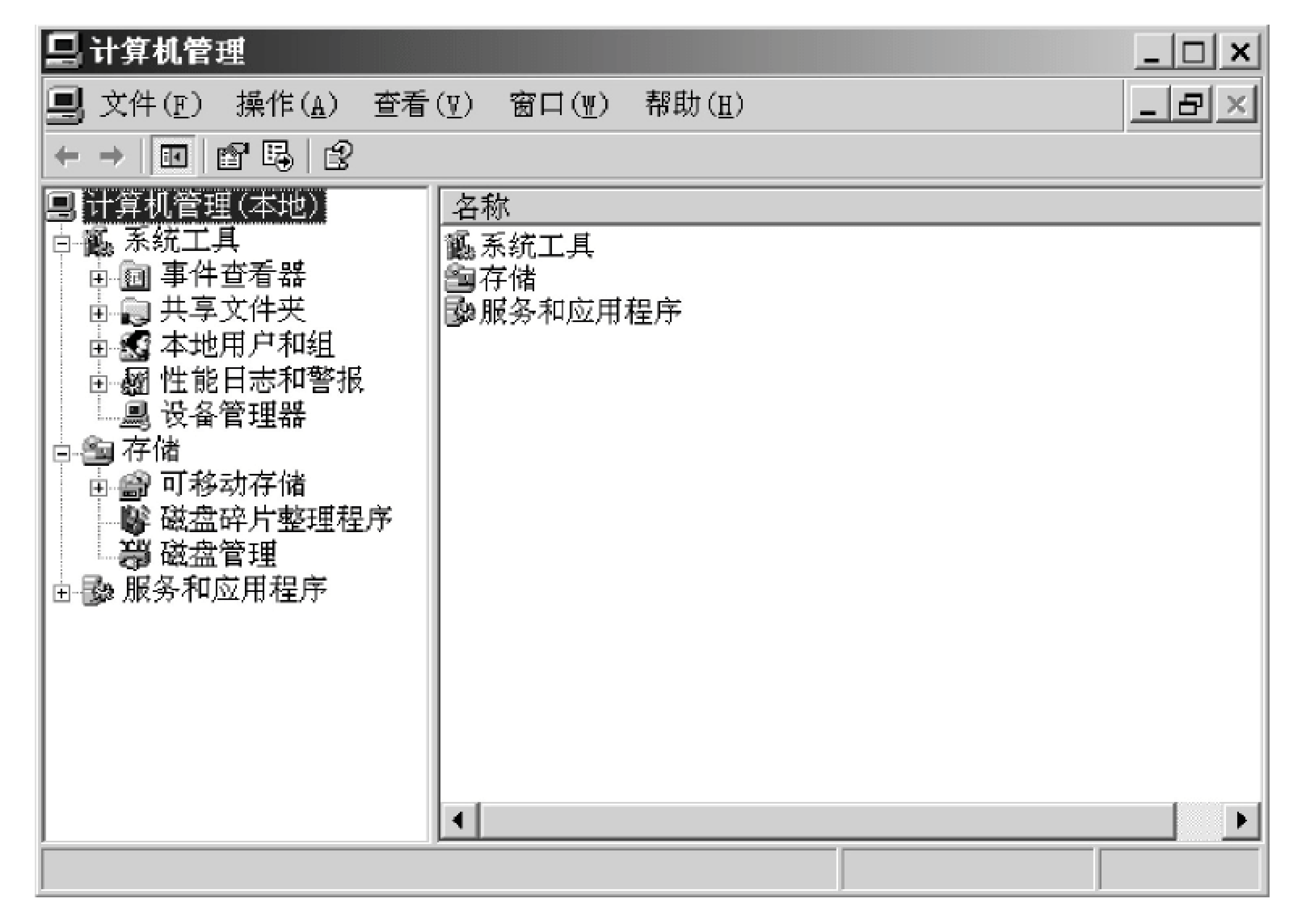


图 4-18 “计算机管理”窗口

别存放本机的用户和组，双击“用户”目录显示用户信息，如图 4-19 所示。

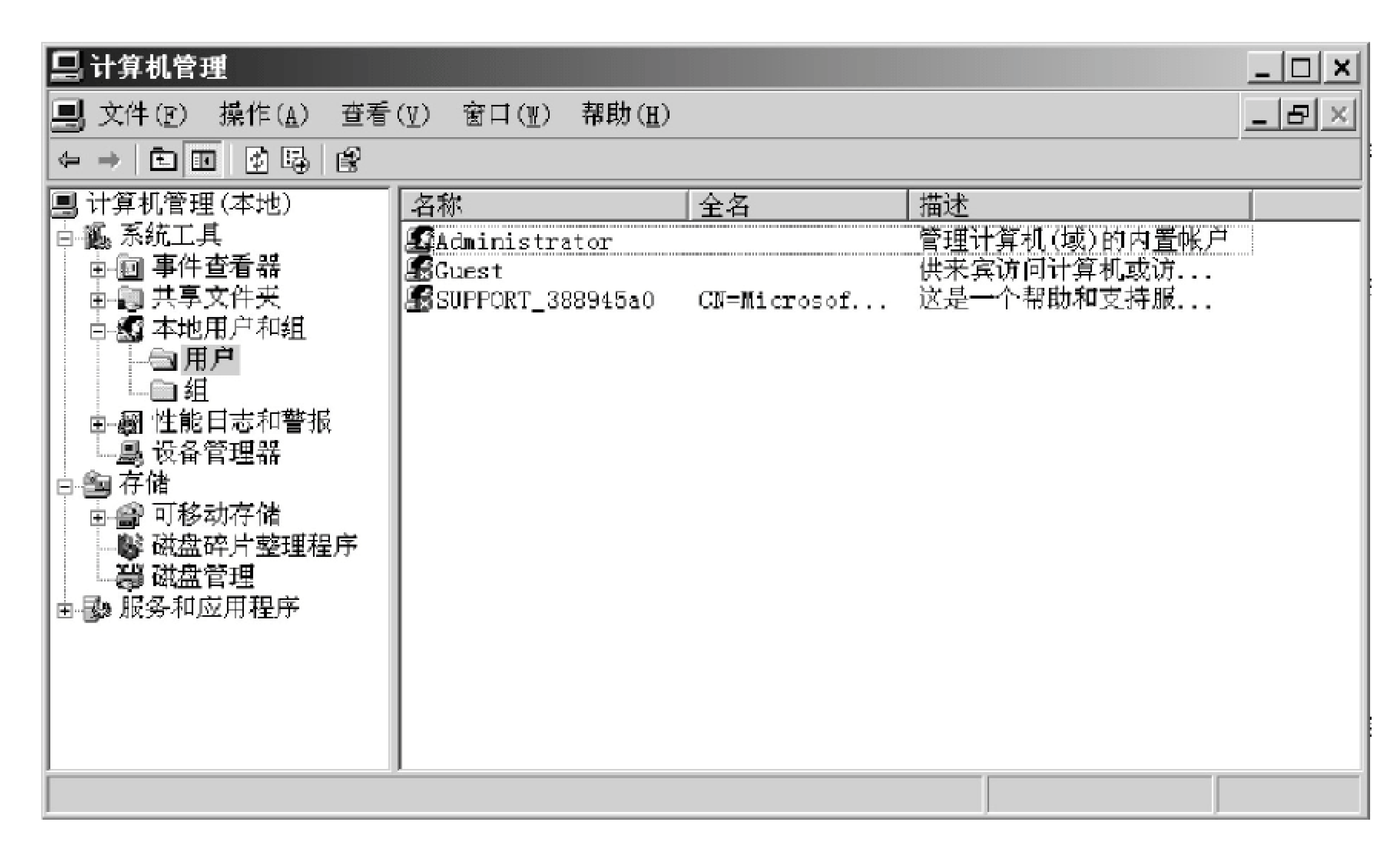
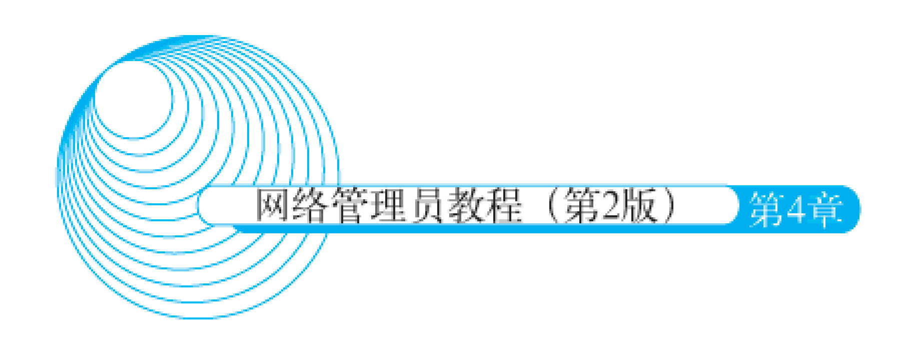


图 4-19 “计算机管理窗口”的用户设置

（3）单击鼠标右键，单击“新用户”，弹出添加新用户的对话框，依次输入用户名、用户全名、描述、密码以及确认密码，在密码属性多选框中选择“用户下次登录时须更改密码”，单击“创建”



按钮，即可创建新用户，如图 4-20 所示。

(4) 采用同样的方法可以进行组的管理，如图 4-21 所示。其中组的名称和权限描述如表 4-2所示。



图 4-20　添加新用户



图 4-21　组的管理

表 4-2　用户权限描述

名称	权限描述
Administrators	管理员对计算机/域有不受限制的完全访问权
Backup Operators	备份操作员为了备份或还原文件可以替代安全限制
Guests	按照默认值，来宾跟用户组的成员有同等访问权，但来宾账户的限制更多
HelpServicesGroup	帮助和支持中心组
Network Configuration Operators	此组中的成员有部分管理权限来管理网络功能的配置
Performance Log Users	此组的成员可以远程访问以计划此计算机上性能计数器的日志
Performance Monitor Users	此组的成员可以远程访问以监视此计算机
Power Users	高级用户(Power Users)拥有大部分管理权限，但也有限制。因此，高级用户可以运行经过验证的应用程序，也可以运行旧版应用程序
Print Operators	成员可以管理域打印机

续表

名称	权限描述
Remote Desktop Users	此组中的成员被授予远程登录的权限
Replicator	支持域中的文件复制
TelnetClients	本组的成员可以访问此系统上的 Telnet 服务器
Users	用户无法进行有意或无意的改动。因此，用户可以运行经过验证的应用程序，但不可以运行大多数旧版应用程序

3. 添加、删除与管理网络服务

安装 Windows Server 2003 时，在默认的情况下并不安装任何网络服务，它只是一个提供用户登录的独立的网络服务器。因此，必须在添加网络服务并进行必要配置后，才能为网络提供各种服务。

1）添加网络服务

可采用两种方式来进行网络服务的添加，分别是通过“管理您的服务器”和“控制面板”。

方式一：通过“管理您的服务器”添加网络服务。操作步骤如下：

（1）启动“管理您的服务器”。默认情况下该操作窗口随系统启动自动打开，用户也可以单击屏幕左下角的“开始”→“所有程序”→“管理工具”→“管理您的服务器”来完成这一步骤。启动后屏幕如图 4-22 所示。

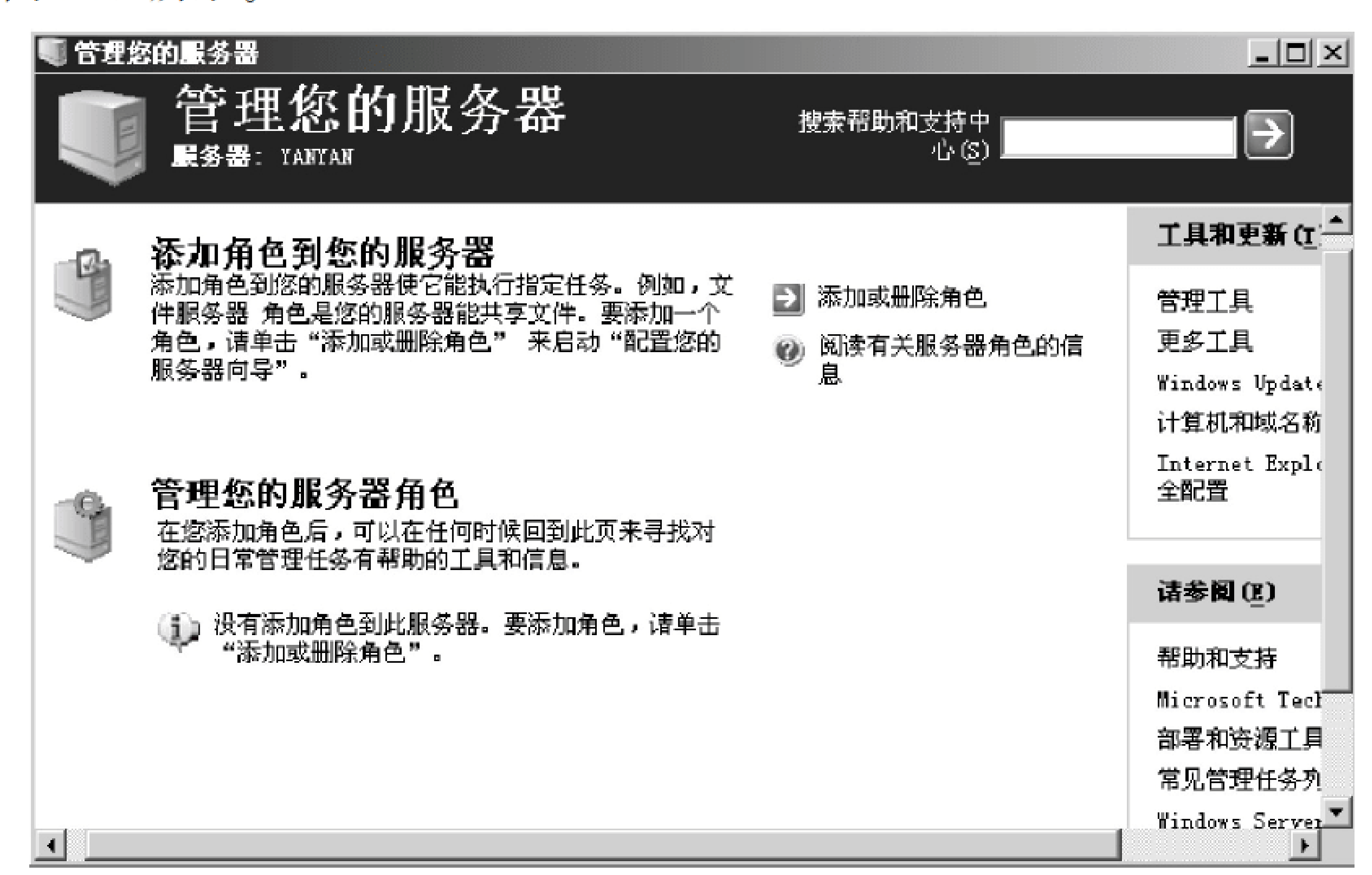
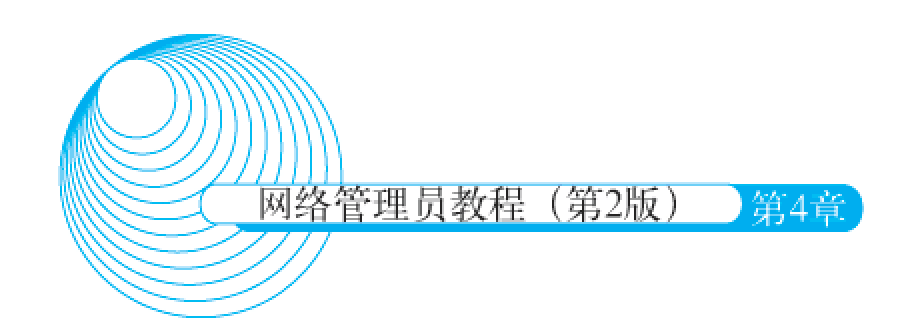


图 4-22 “管理您的服务器”启动窗口



（2）在“管理您的服务器”窗口中依次单击“添加或删除角色”→“下一步”按钮，系统将自动检查网络配置并做好服务器安装前的准备，如图 4-23 所示。

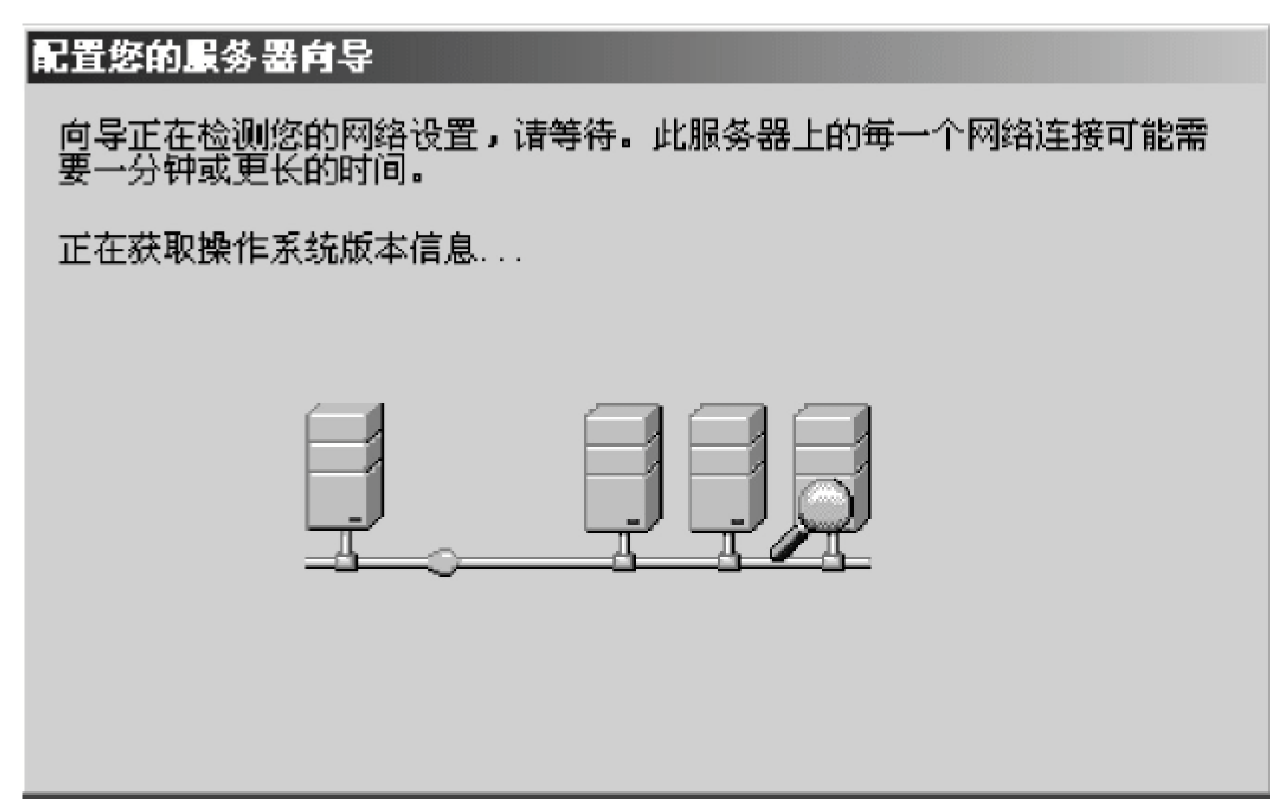


图 4-23　配置服务器向导

（3）网络配置检查完毕，显示如图 4-24 所示的“服务器角色”对话框，此时所有可安装的网络服务全显示在列表框中。“已配置”列表框说明该网络服务是否已经安装。在列表中选择准备安装的服务，单击“下一步”按钮。

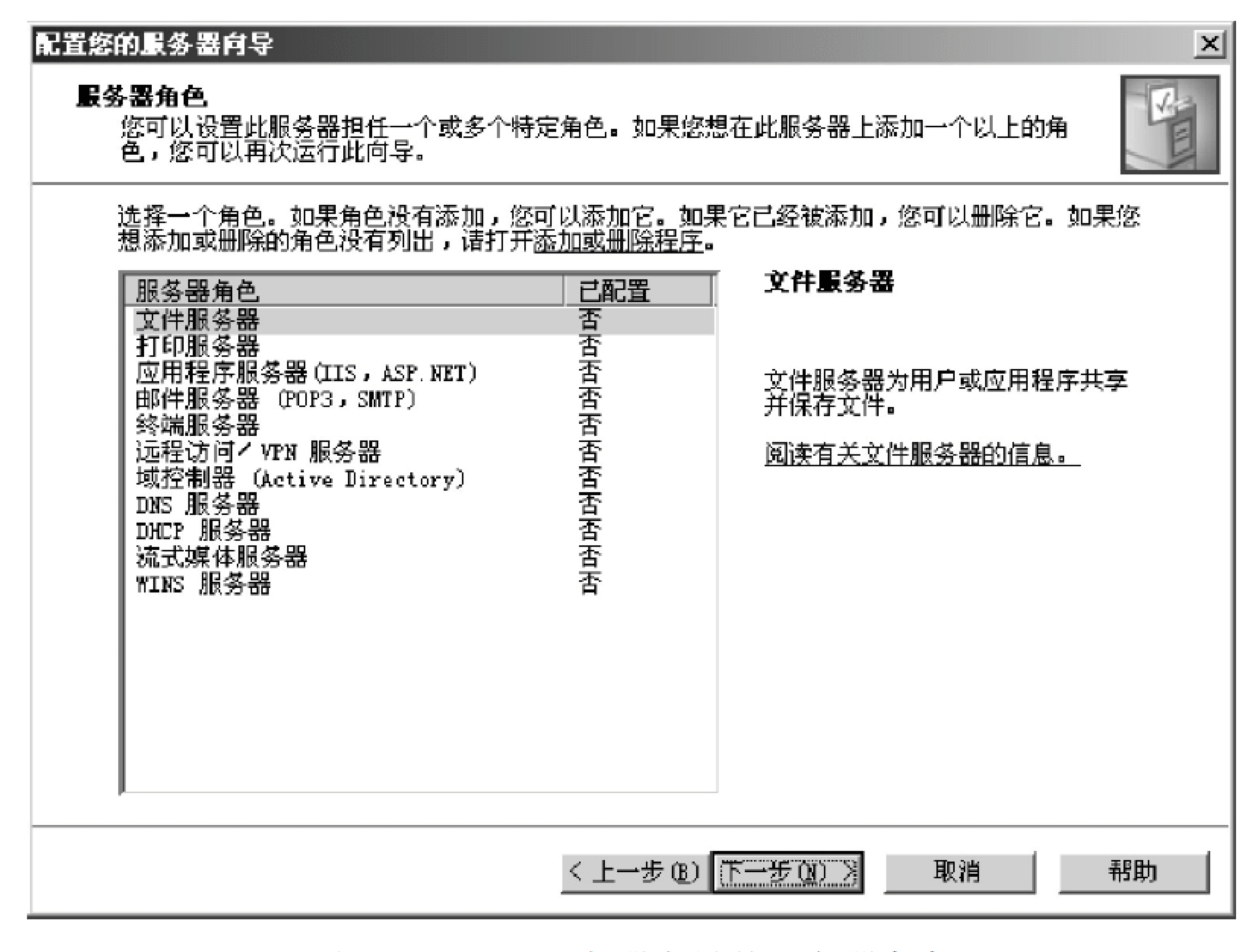


图 4-24　配置服务器向导的服务器角色

（4）系统根据用户选择的服务提示用户插入系统安装盘，根据配置向导进行一些简单的服务配置。如图 4-25 所示的是 DHCP 的配置。安装完成后返回“管理您的服务器”窗口，将显示已经安装的网络服务。



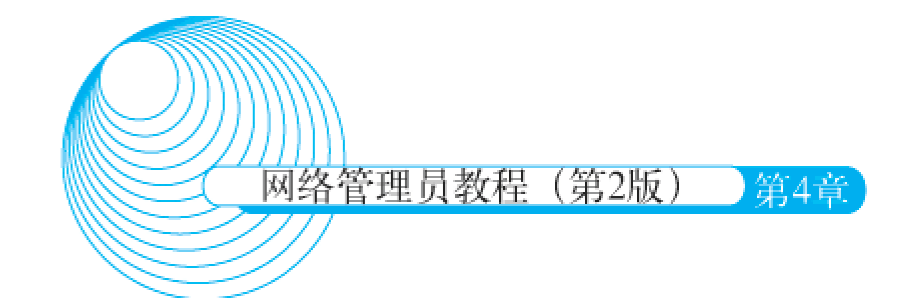
图 4-25　安装 DHCP 服务器

方式二：通过“添加/删除 Windows 组件”添加网络服务。操作步骤如下：

（1）在系统“控制面板”中双击“添加或删除程序”，弹出如图 4-26 所示的窗口。



图 4-26　“添加或删除程序”窗口



（2）单击窗口中左侧的“添加/删除 Windows 组件”按钮，双击“添加或删除程序”，系统将出现一个检测信息框自动搜集 Windows 组件信息，随后弹出如图 4-27 所示的窗口，有些服务就位于“Windows 组件向导”对话框的“组件”列表中，例如 Internet Explorer 增强的安全配置、Windows Media Services、电子邮件服务、UDDI 服务等，如果需要安装某种服务，直接选中它前面的复选框。然后单击“下一步”按钮。



图 4-27 “Windows 组件向导”对话框

有些服务比如 DHCP、DNS 等属于“网络服务”组件，如要安装需在列表中选中“网络服务”复选框，然后再单击“详细信息”按钮，在“网络服务”对话框中选择要安装的服务，如图 4-28 所示。

（3）插入系统安装盘，根据提示依次单击“确定”按钮进行安装。这种安装方式不会自动调用相关的服务器配置向导，需要在成功安装后再进行手工配置。

2）删除网络服务

方式一：通过“管理您的服务器”删除网络服务。操作步骤如下：

（1）打开“管理您的服务器”窗口，如图 4-22 所示，依次单击“添加或删除角色”按钮和“下一步”按钮。

（2）在“服务器角色”对话框中选中所要删除的网络服务复选框，如图 4-29 所示，单击“下一步”按钮。

（3）选中“删除 DNS 服务器角色”的复选框，单击“下一步”按钮即可删除 DNS 网络服务，如

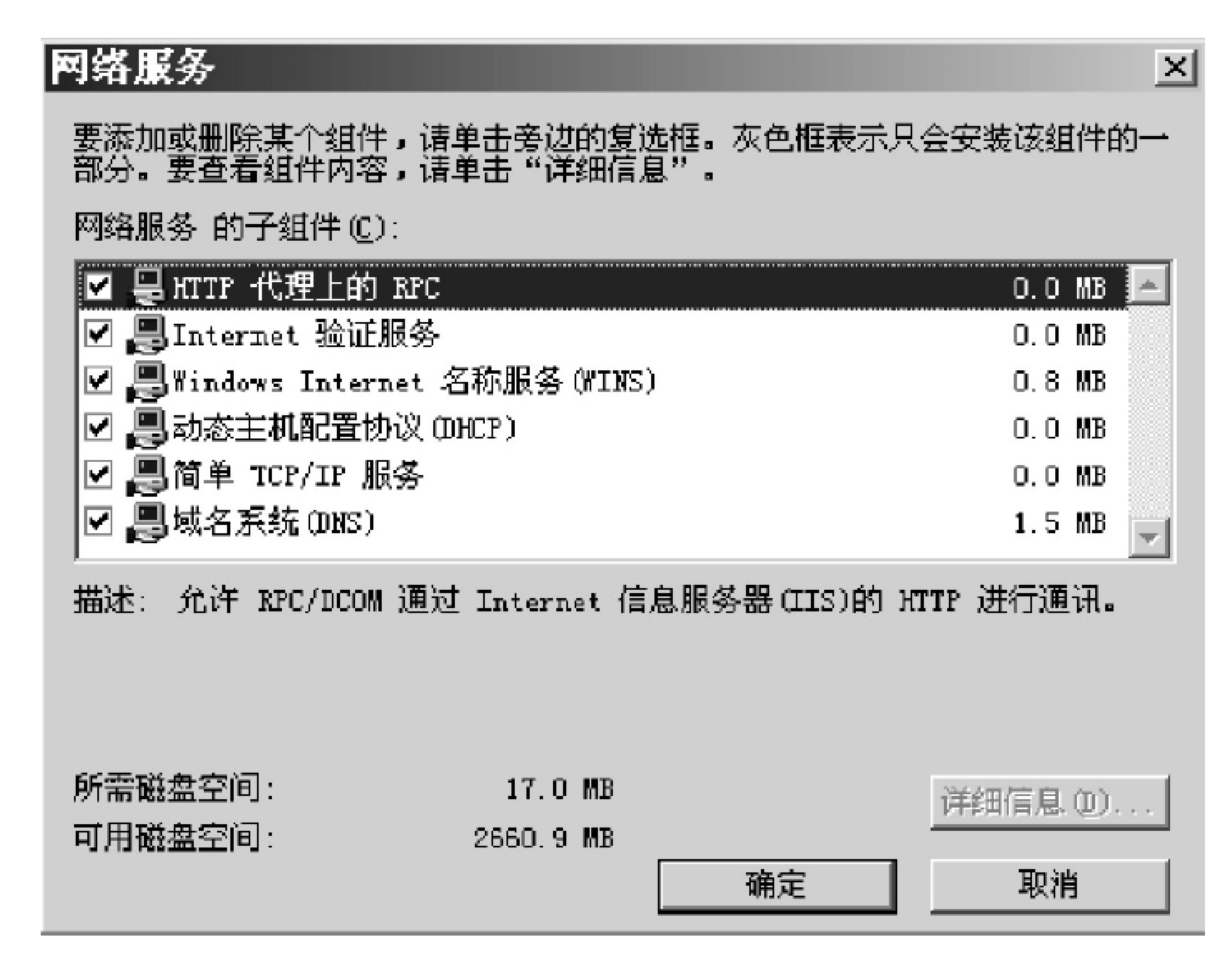


图 4-28 “网络服务”对话框

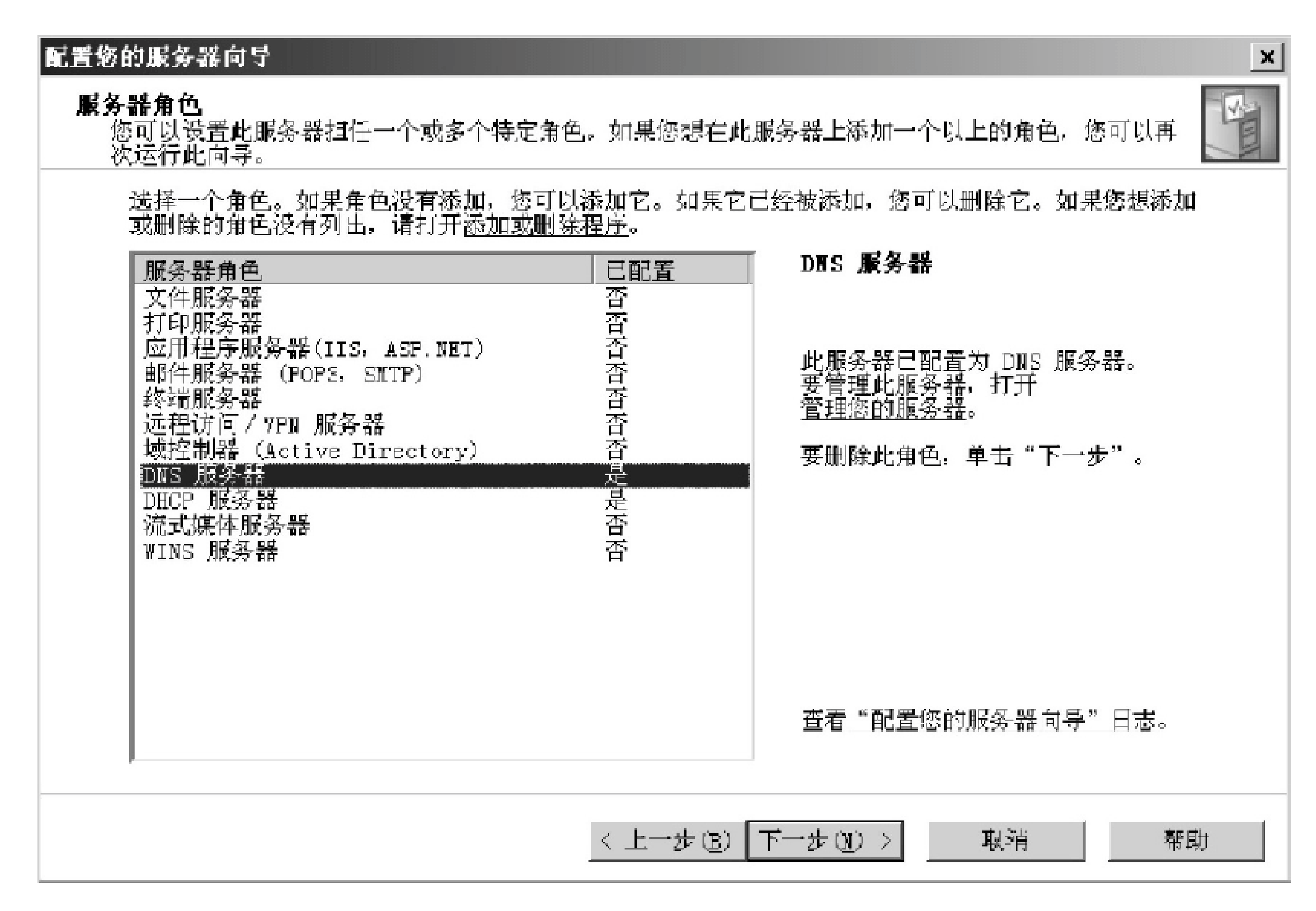


图 4-29 配置服务器向导的服务器角色——删除 DNS 服务器角色

图 4-30 所示。

方式二：通过“添加/删除 Windows 组件”删除网络服务。操作方法如下：

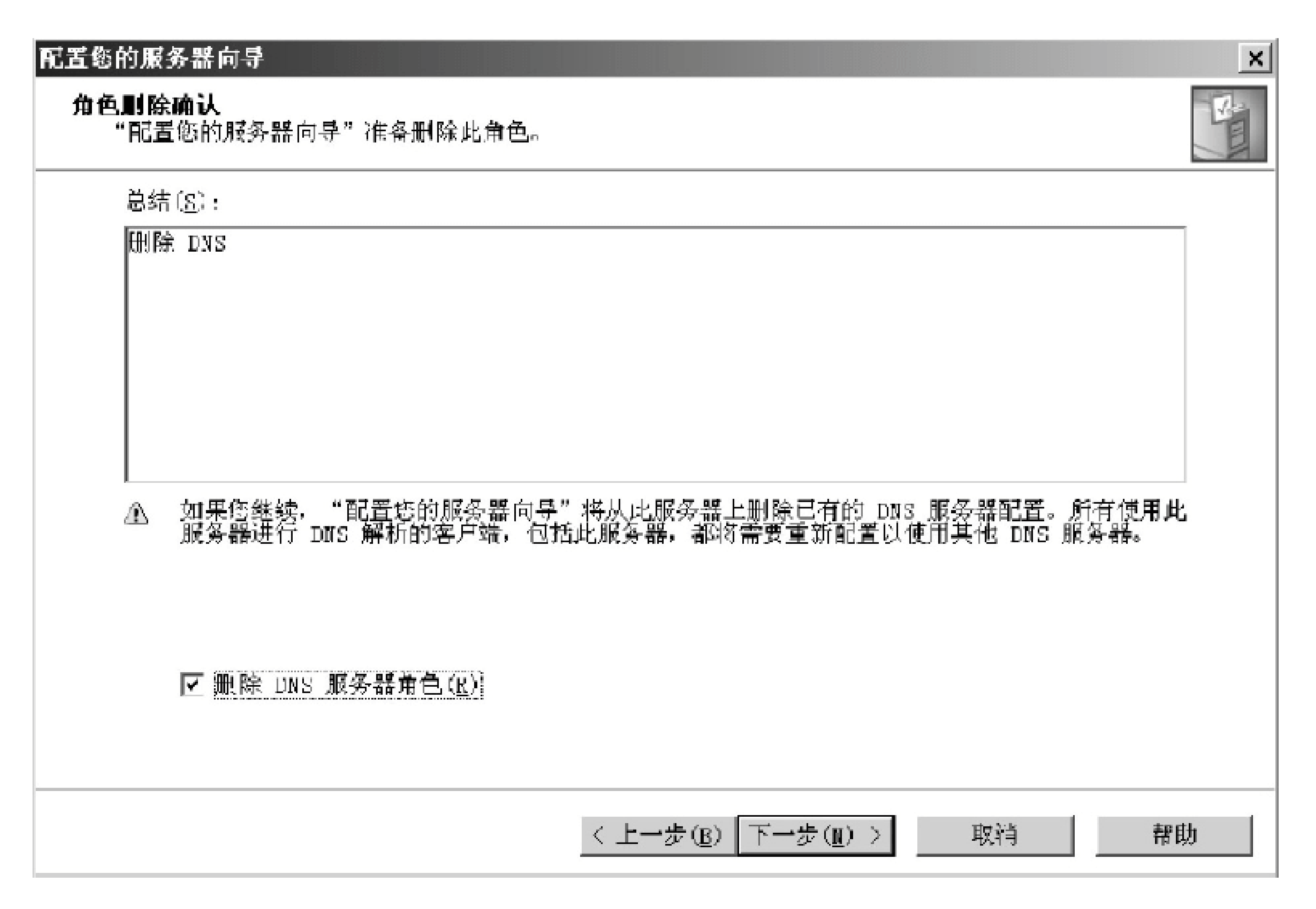


图 4-30　角色删除确认

运行“添加/删除 Windows 组件”向导，在“Windows 组件”对话框的“组件”列表框或“网络服务”对话框中，取消欲删除服务的复选框，如图 4-31 所示，依次单击“确定”按钮即可。

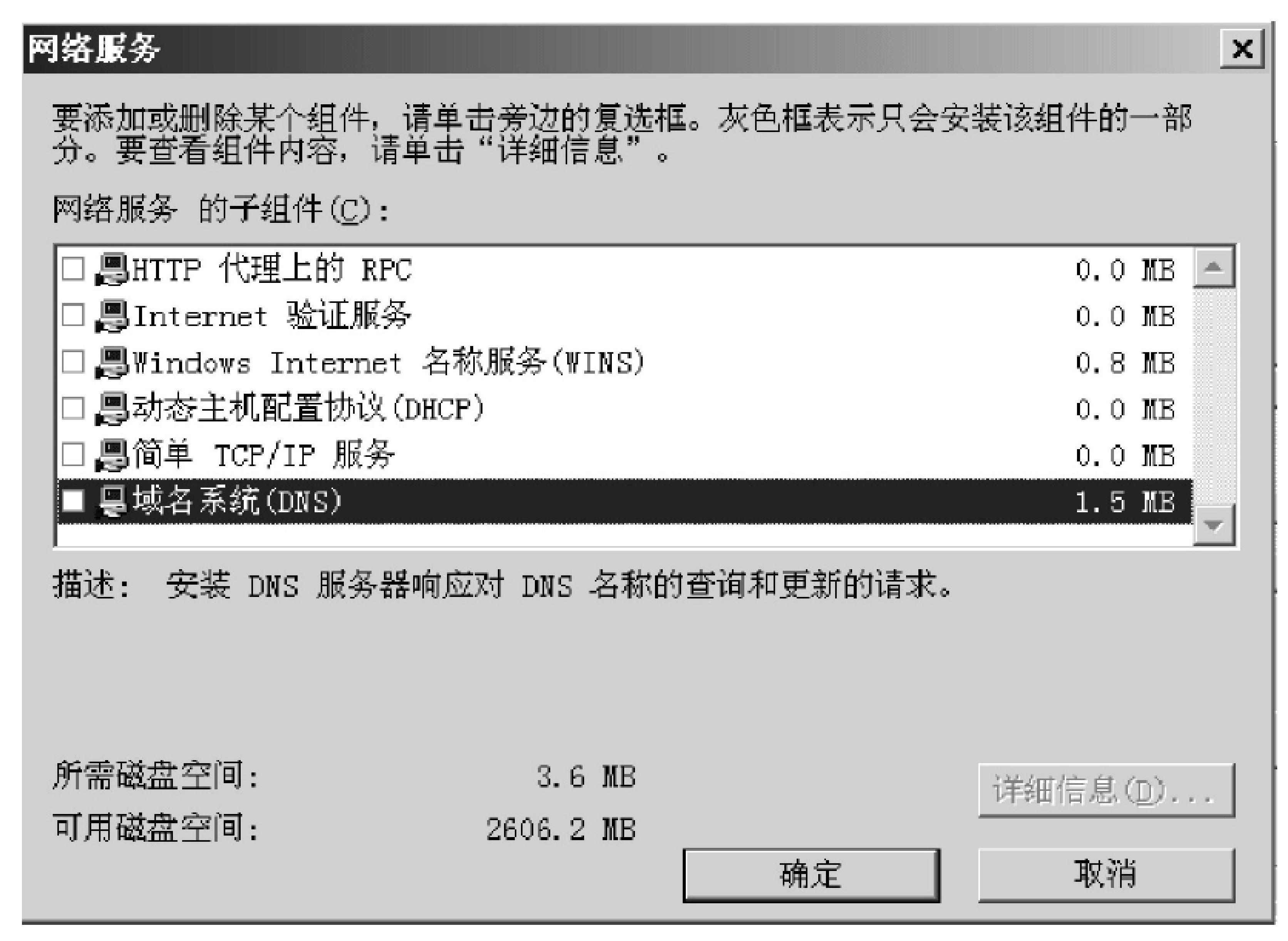


图 4-31　“网络服务”对话框——添加或删除组件

4. 配置网络协议

只有在计算机上正确安装网卡驱动程序和网络协议，并正确设置 IP 地址信息之后，服务器才能与网络内的计算机进行正常通信。

1）安装网卡

Windows Server 2003 支持即插即用功能，并且内置了很多知名品牌网卡的驱动程序。因此在正常情况下，安装 Windows Server 2003 时系统就已经自动完成了网卡的安装。

如果系统没有提供网卡的相应驱动程序。在安装好 Windows Server 2003 系统之后，依次单击"开始"→"程序"→"管理工具"→"计算机管理"，在控制台中单击"设备管理器"，展开"其他设备"，显示"以太网控制器"，右击控制器在快捷菜单中选择"卸载"以卸载未成功安装的网卡，然后选择"扫描硬件改动"，依照系统提示插入网卡驱动程序盘，依次单击"下一步"按钮进行安装。

2）配置 IP 地址信息

在 Windows Server 2003 系统中，若正确安装了网卡等网络设备，系统可自动安装 TCP/IP 协议。TCP/IP 协议的配置操作步骤如下：

（1）依次单击"开始"→"控制面板"→"网络连接"→"本地连接"选项，将出现如图 4-32 所示的对话框。

（2）单击"属性"按钮，将显示"本地连接属性"对话框，如图 4-33 所示。

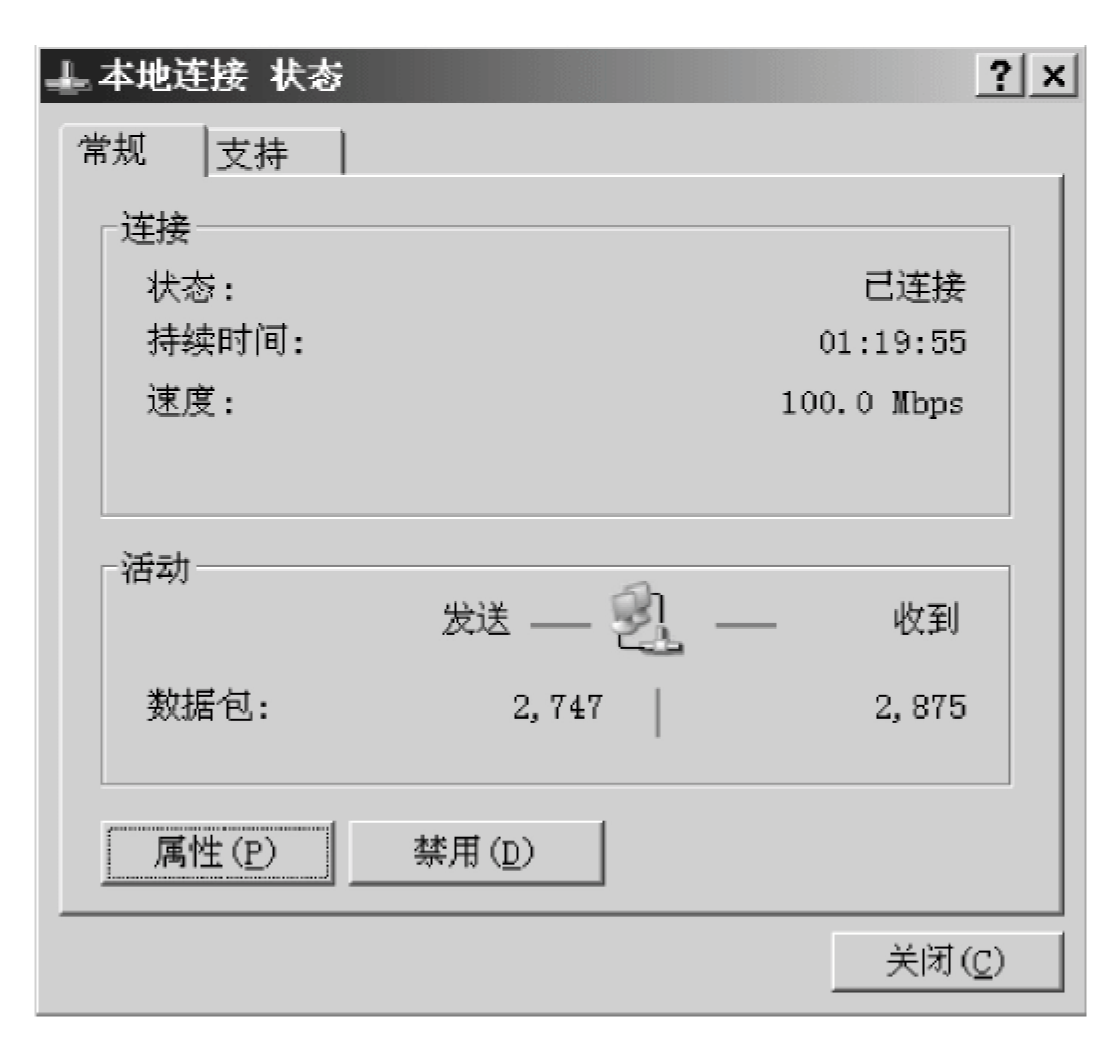


图 4-32 "本地连接状态"对话框



图 4-33 "本地连接属性"对话框

（3）在列表中选择“Internet 协议（TCP/IP）”选项，单击“属性”按钮，或者双击列表中“Internet 协议（TCP/IP）”选项，系统弹出如图 4-34 所示的“Internet 协议（TCP/IP）”属性对话框。

（4）分别在文本框中输入 IP 地址、子网掩码、默认网关以及 DNS 服务器的 IP 地址等信息。有关 DNS、WINS 等的高级设置，单击“高级”按钮进行设置，如图 4-35 所示。

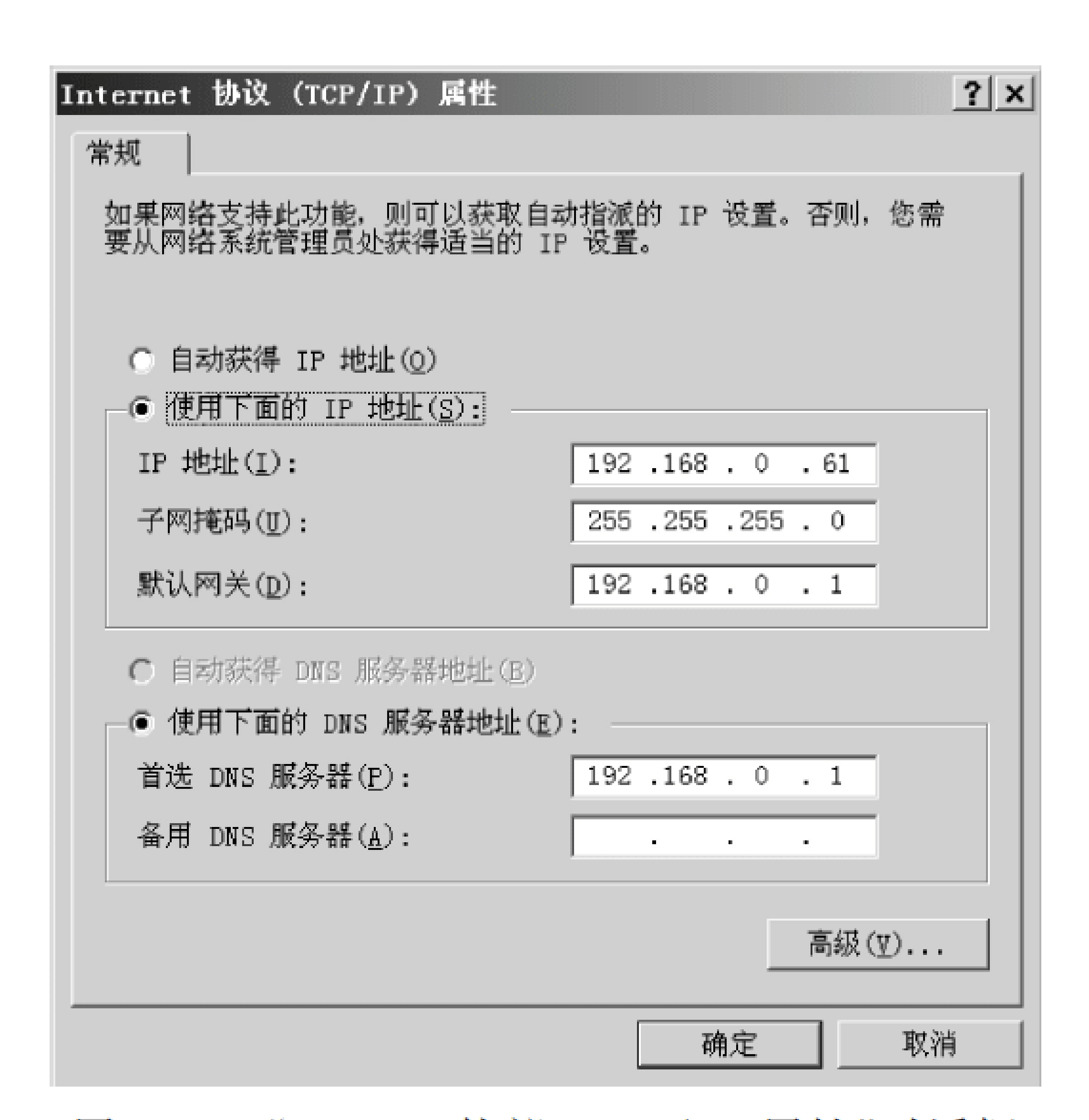


图 4-34 “Internet 协议（TCP/IP）属性”对话框

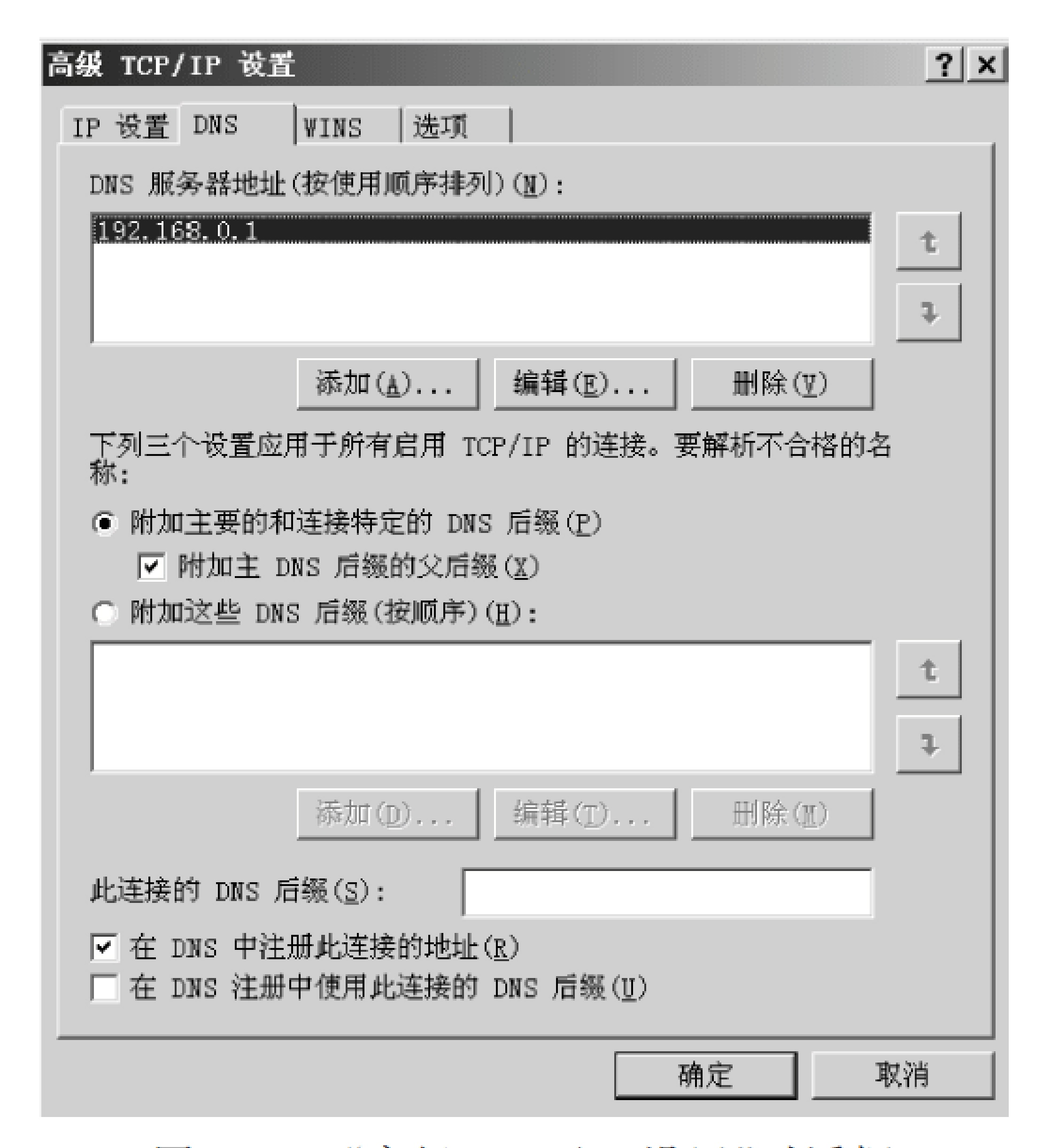


图 4-35 “高级 TCP/IP 设置”对话框

5. 配置文件服务器

文件服务器提供并管理对文件的访问。在 Windows Server 2003 中，默认状态下并没有安装文件服务器，需要手工搭建，具体的操作步骤如下：

（1）在“管理您的服务器”窗口中单击“添加或删除角色”，系统显示“配置您的服务器向导”窗口，单击“下一步”按钮，服务器配置向导检测网络配置，然后显示“服务器角色”配置向导，在列表框中选中“文件服务器”，如图 4-36 所示，单击“下一步”按钮。

（2）在出现的“文件服务器磁盘配额”对话框中，选中“为此服务器的新用户设置默认磁盘空间配额”复选框，如图 4-37 所示。为“将磁盘空间限制为”和“将警告级别设置为”两个选项设置数值，然后单击“下一步”按钮。当用户使用的空间达到指定的警告值时，系统提示用户磁盘空间不足；当用户使用的空间达到规定的磁盘限额时，系统将禁止用户再向服务器写入文件，从而确保服务器空间的合理使用，避免服务器的滥用。

（3）在系统显示的“文件服务器索引服务”对话框中，选中“是，启用索引服务”单选按钮，以

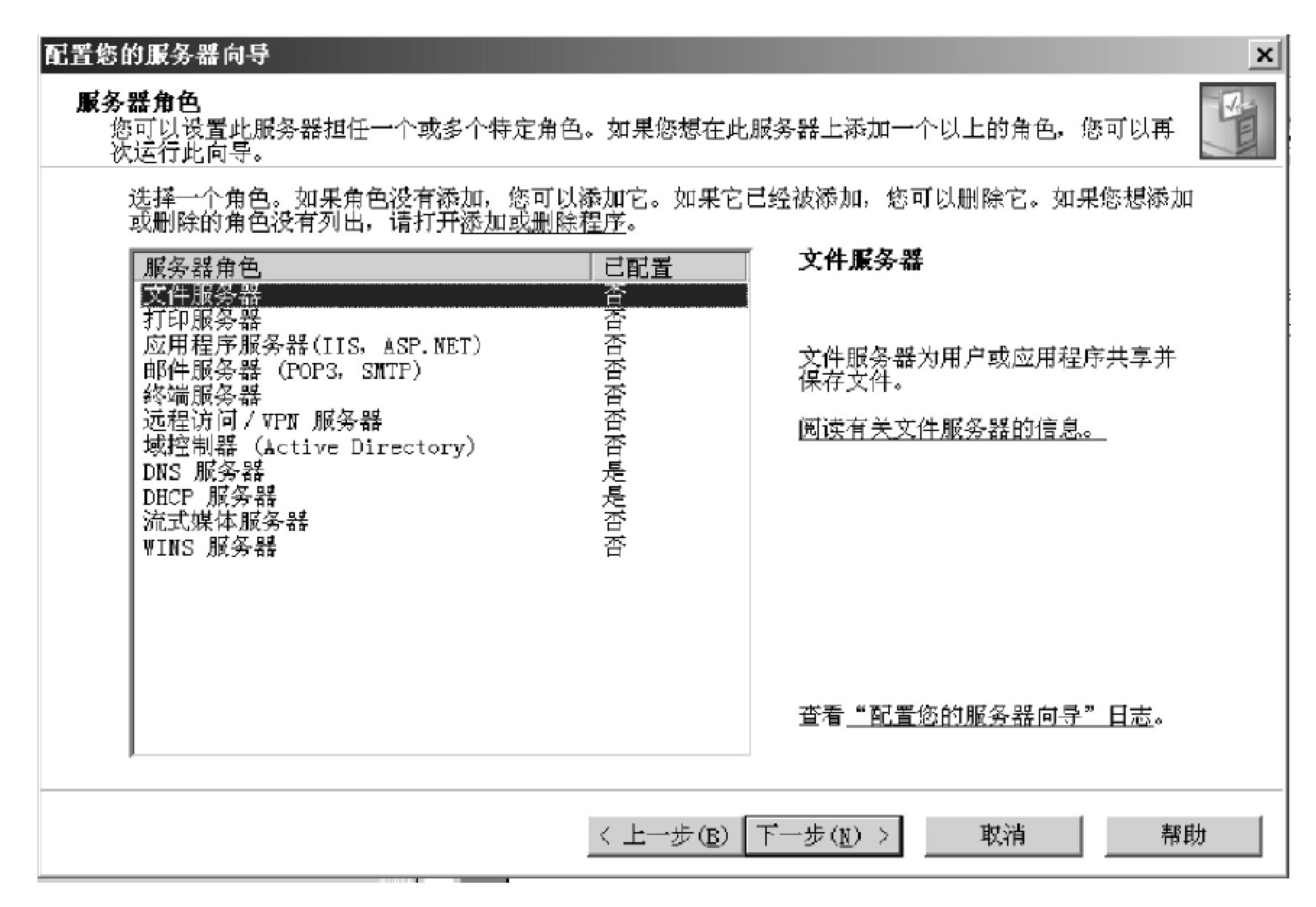


图 4-36　文件服务器安装

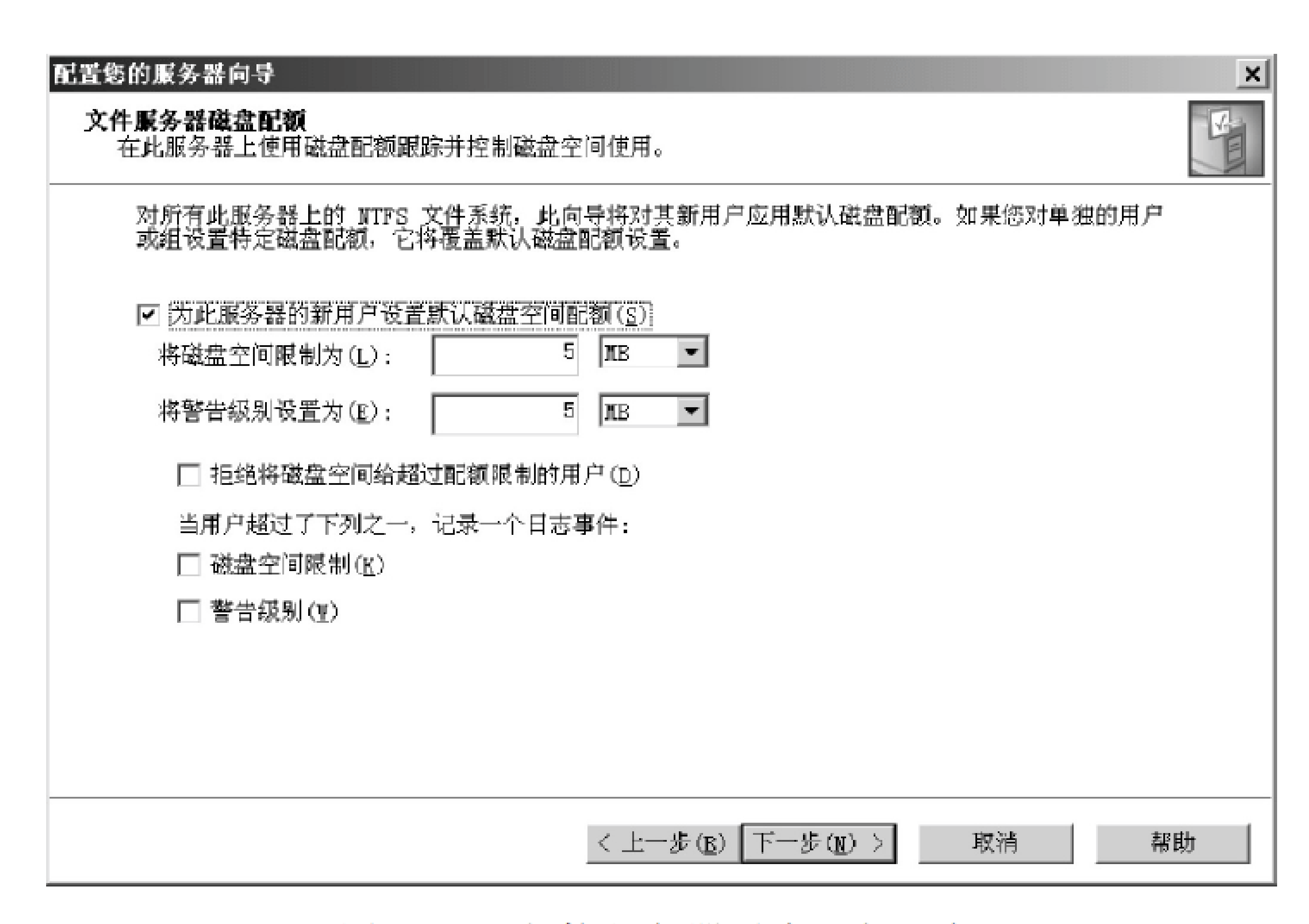


图 4-37　文件服务器磁盘空间配额

启用对共享文件夹的索引服务，然后单击“下一步”按钮，如图 4-38 所示。因为启用索引服务将占用大量的服务器资源，从而导致服务器的性能下降，因此只有用户经常在该服务器上搜索文件时才启用该索引。

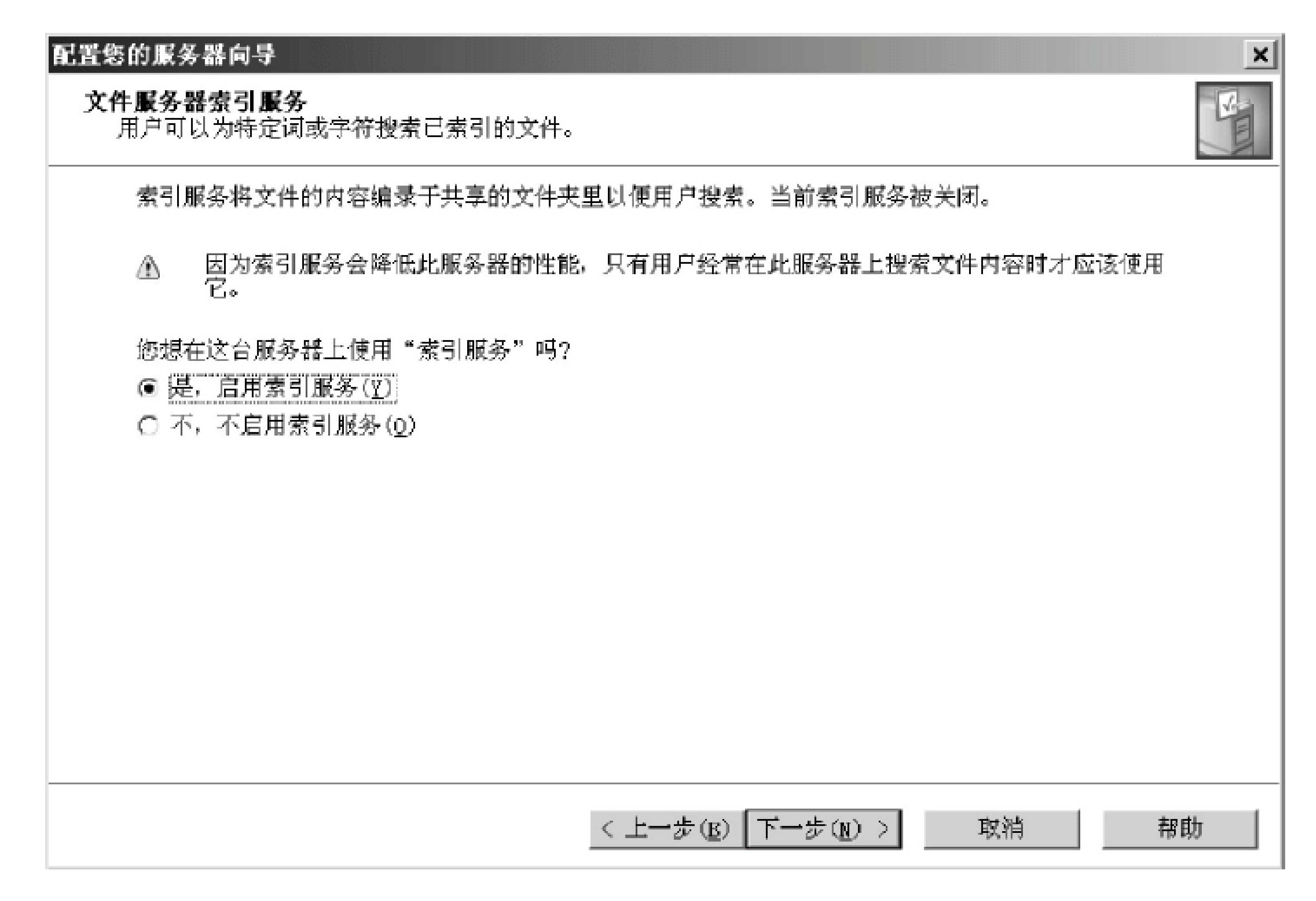


图 4-38 “文件服务器索引服务”配置对话框

（4）系统出现“选择总结”对话框，在这里列出了对文件服务器已经作出的选择。若欲修改某项设置，请单击“上一步”按钮返回修改，然后单击“下一步”按钮，如图 4-39 所示。此时系统将自动进行配置。同时，启动“共享文件夹向导”。

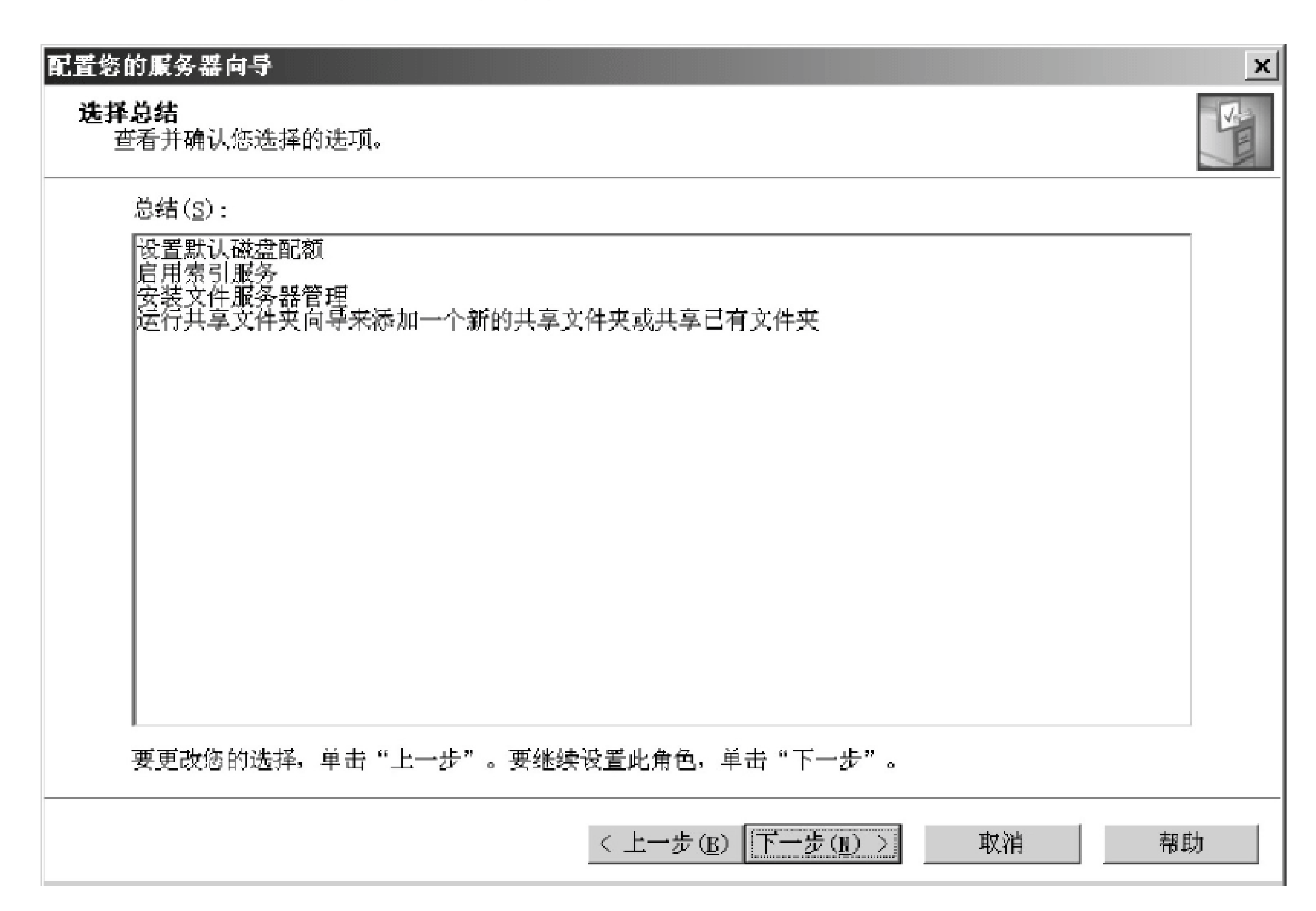


图 4-39 “选择总结”对话框

（5）在“共享文件夹向导”的“文件夹路径”对话框中，在“文件夹路径”中直接输入路径或通过“浏览”查找预共享的文件夹，然后单击“下一步”按钮，如图 4-40 所示。



图 4-40　“共享文件夹路径”配置对话框

（6）在弹出的“名称、描述和设置”对话框中，填写共享名和描述信息，然后单击“下一步”按钮，如图 4-41 所示。其中“共享名”是显示给用户的文件夹名，“描述”是关于该文件夹的描述，为方便用户而设置的。

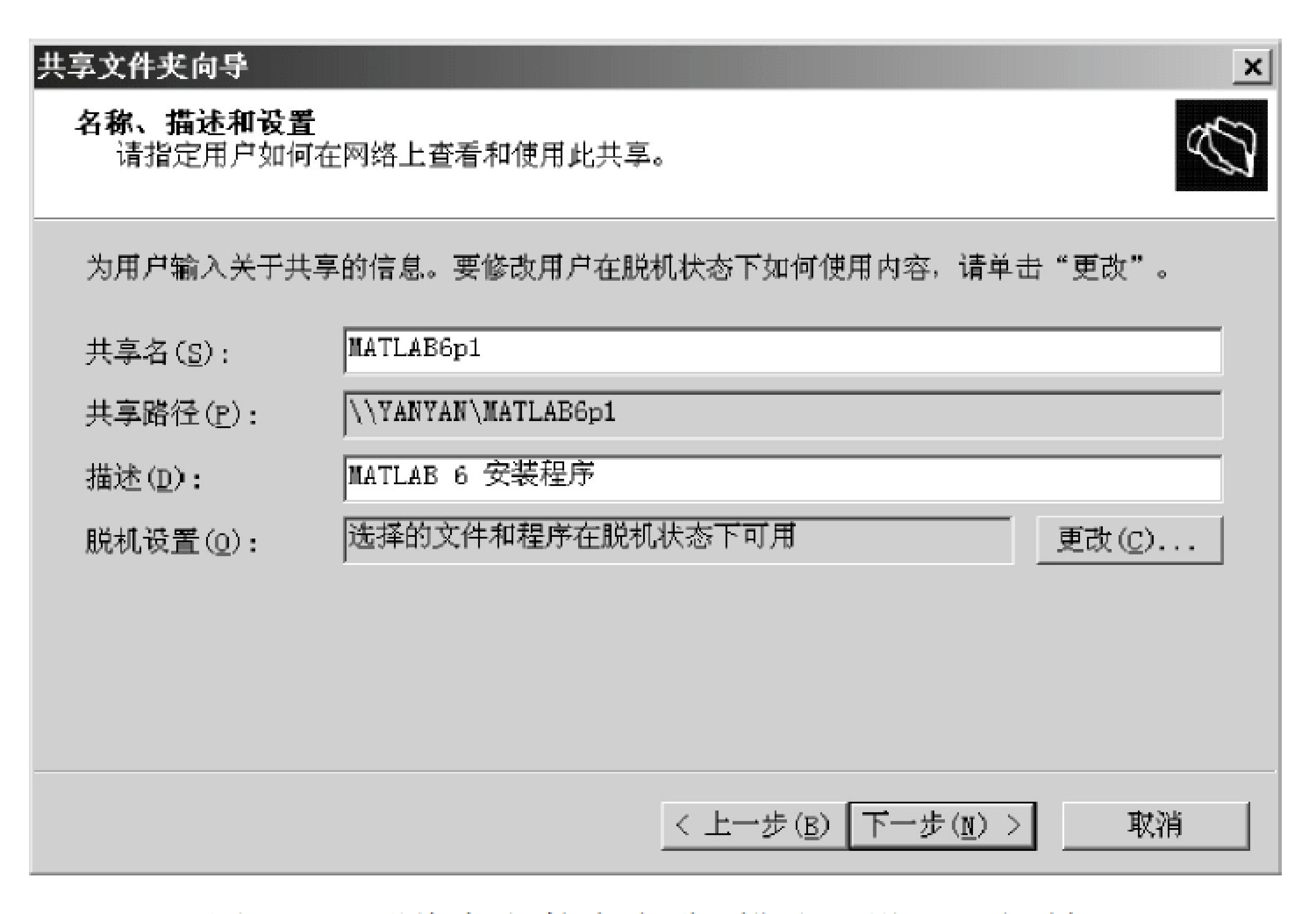
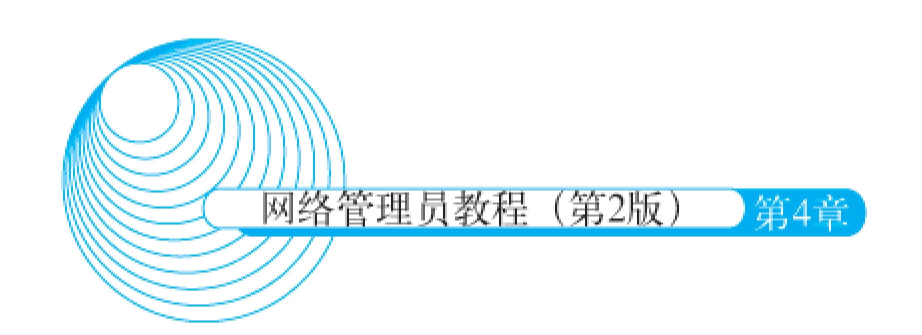


图 4-41　“共享文件夹名称、描述和设置”对话框



（7）在弹出的“权限”对话框中，根据可供使用的权限，选择一个选项，然后单击“完成”按钮，如图 4-42 所示。

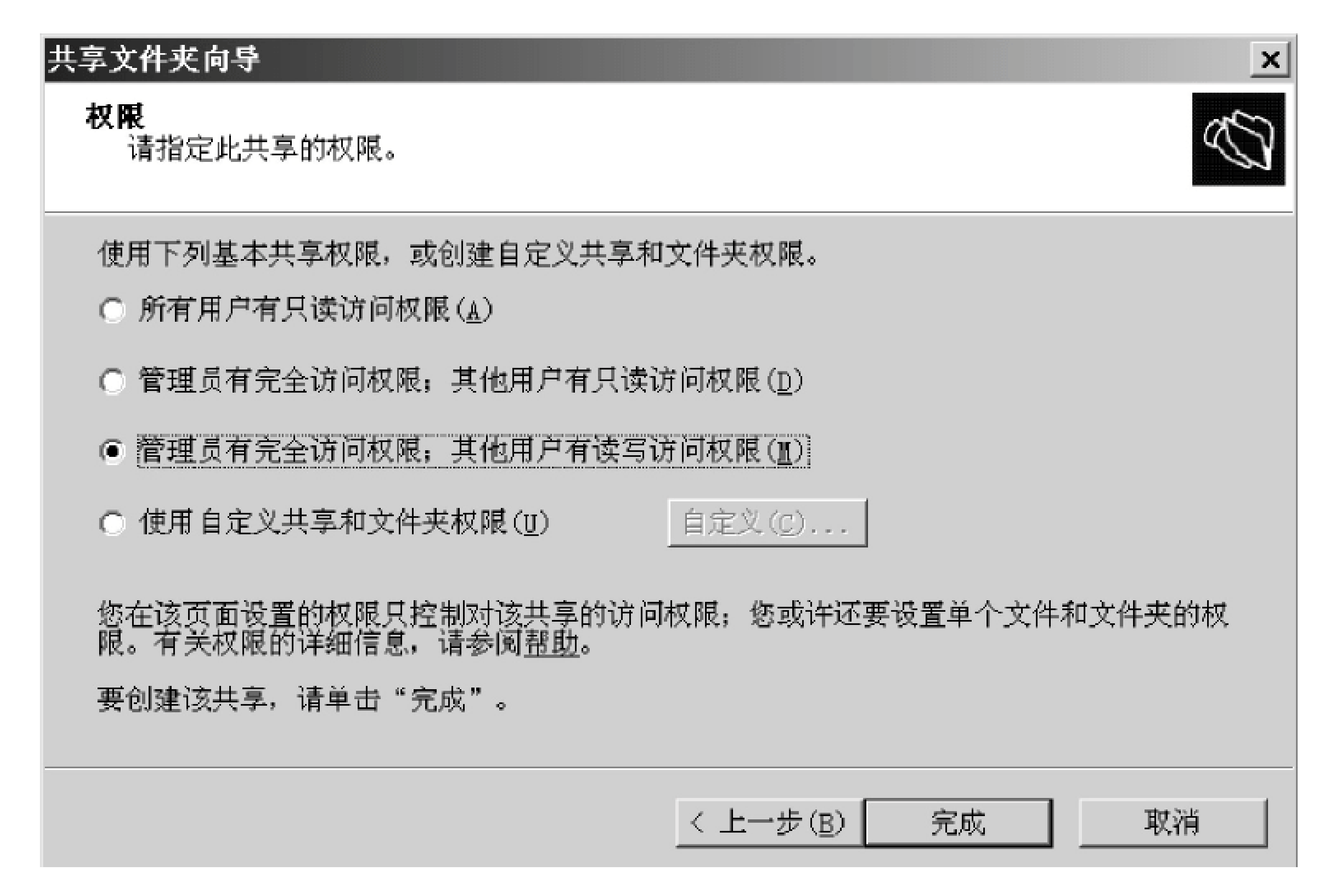


图 4-42　共享文件夹“权限”设置对话框

（8）系统显示“共享成功”对话框，并在摘要中列出了该共享文件夹的参数信息，至此共享文件夹设置成功，单击“关闭”按钮，如图 4-43 所示。

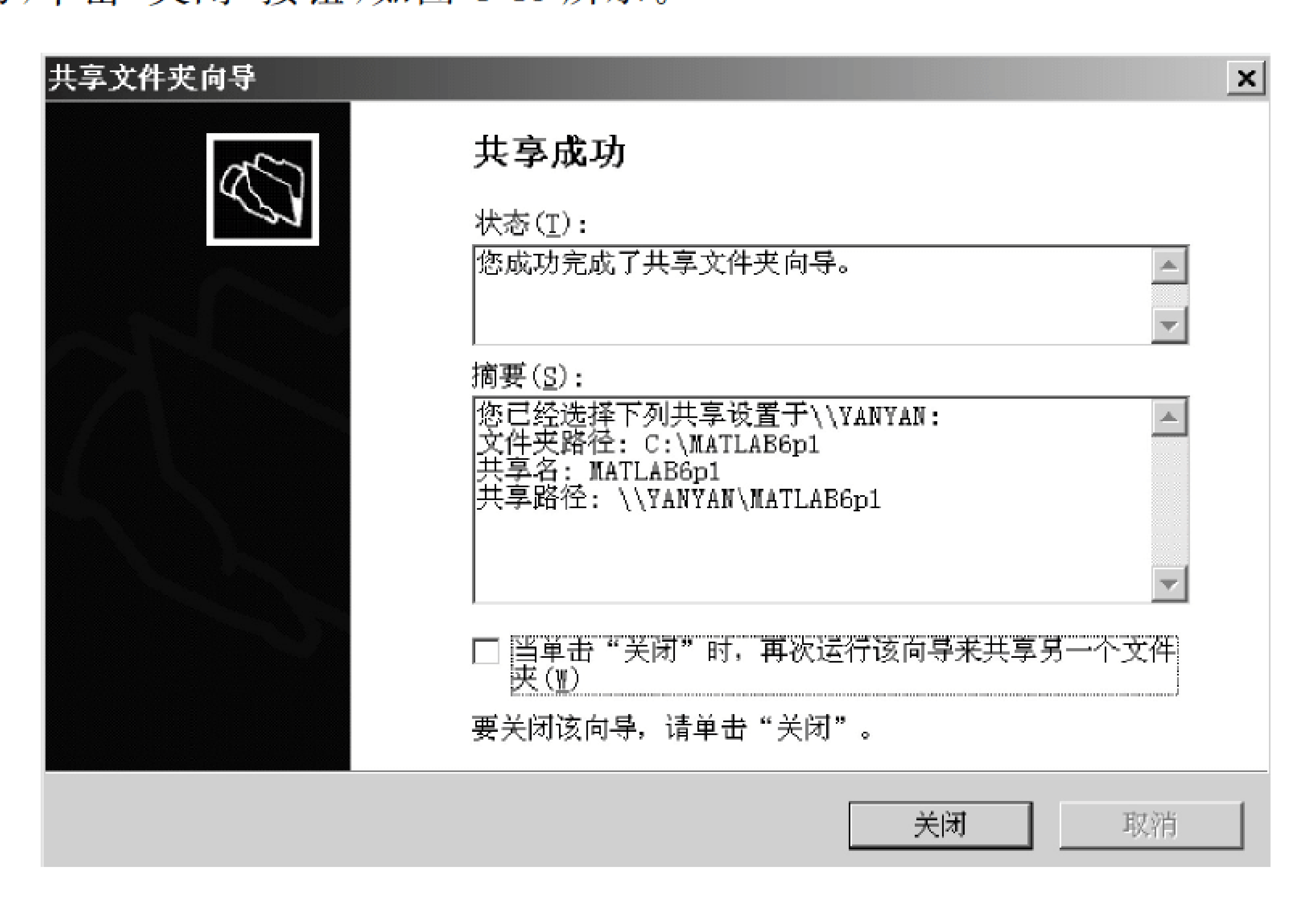


图 4-43　共享文件夹“共享成功”对话框

6. 终端服务

1）终端服务概述

终端服务提供了通过作为终端仿真器工作的“瘦客户机”软件远程访问服务器桌面的能力。终端服务基本由3部分技术组成，即客户端部分、协议部分及服务器端部分。客户端和服务器通过远程桌面协议进行通信。

终端服务的工作方式为，与终端服务相距很远的客户端用户可以像坐在终端服务器前一样执行操作和使用远程终端服务。客户端把键盘输入、鼠标移动和鼠标单击信息发送给终端服务；终端服务得到这些信息，在终端服务的会话内完成所需的操作，然后将更新后的信息发送回客户端。

2）终端服务的安装

在Windows Server 2003中，默认情况下没有安装终端服务，需要进行手动添加，终端服务的安装步骤如下：

(1) 依次单击“开始”→“管理工具”→“配置您的服务器向导”选项。

(2) 单击“下一步”按钮，显示“预备步骤”，提示调制解调器、网卡、电缆、外设以及有无Windows Server 2003安装盘等情况。

(3) 单击“下一步”按钮，显示“检测对话框”，主要检测所有设备、操作系统以及网络连接。检测完成后，出现“配置选项”对话框，选择“自定义配置”选项。

(4) 单击“下一步”按钮，显示“服务器角色”页面，在列表中选择“终端服务器”。

(5) 单击“下一步”按钮，系统显示“选择总结”页面，“选择总结”页面显示了之前所作的选择。

(6) 单击“下一步”按钮，开始安装终端服务器，显示重启计算机提示框。

(7) 单击“确定”按钮，系统将所选择的角色添加到服务器，完成后自动重启计算机，安装完成后的终端服务器如图4-44所示。

3）终端服务的配置与管理

默认情况下只有系统管理员组用户(Administrators)和系统组用户(SYSTEM)拥有访问和完全控制终端服务器的权限，另外远程桌面用户组(Remote Desktop Users)的成员只拥有访问权限而不具备完全控制权。而在很多时候，默认的权限设置往往并不能完全满足实际需求，因此还需要赋予某些特殊用户远程连接的权限。具体设置步骤如下：

(1) 依次单击“开始”→“程序”→“管理工具”→“终端服务配置”选项，显示如图4-45所示的“终端服务配置”窗口。

(2) 单击树型列表框中的“连接”选项，右击右侧列表框中的RDP-Tcp，选择“属性”选项，单击“权限”选项卡，该选项卡对管理员Administrator的访问权限进行了一定的限制；管理员可以

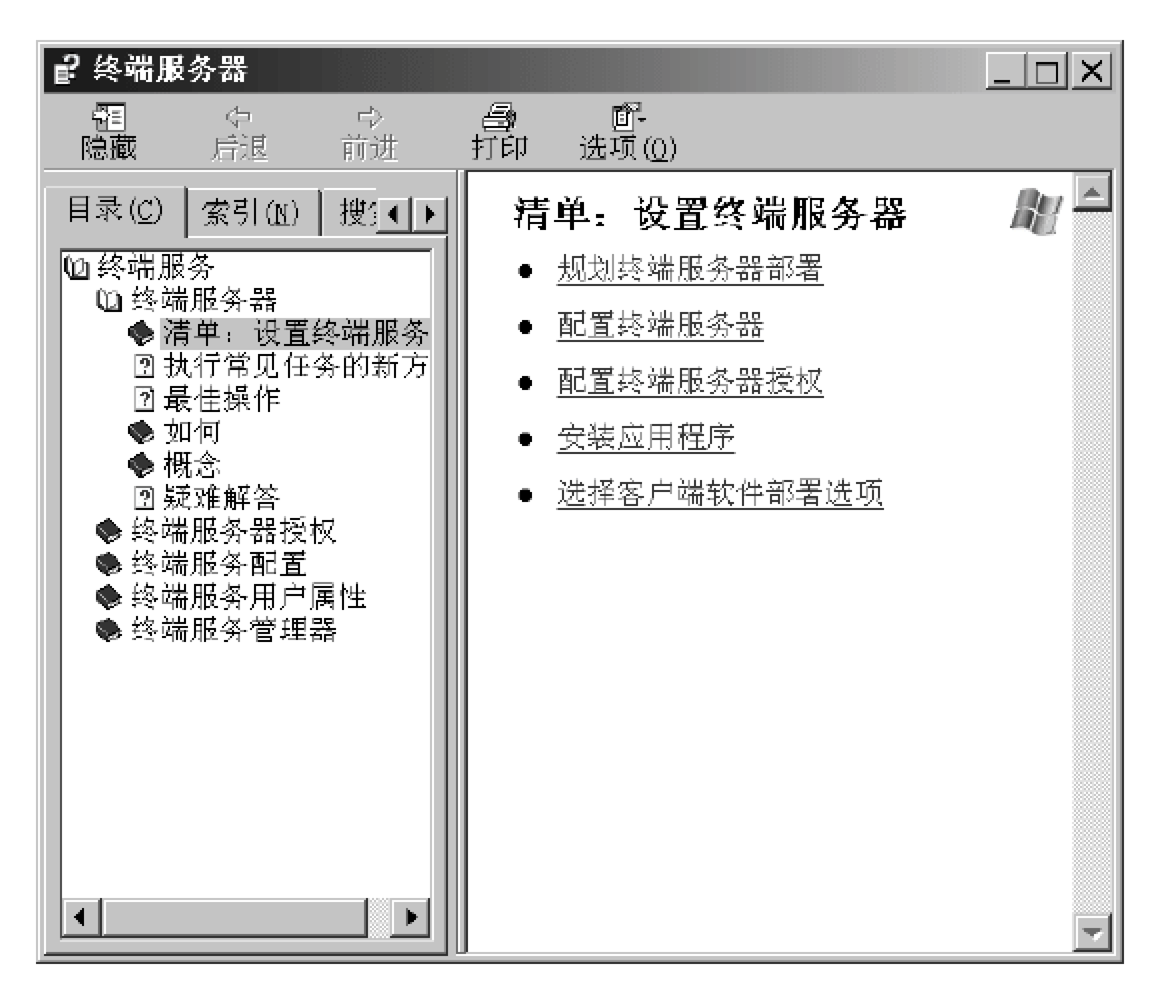


图 4-44　安装完成后的终端服务器

有“完全控制”、“用户访问”以及“来宾访问”3 种权限，通过选中或取消各项的复选框来确定相应的权限，如图 4-46 所示。

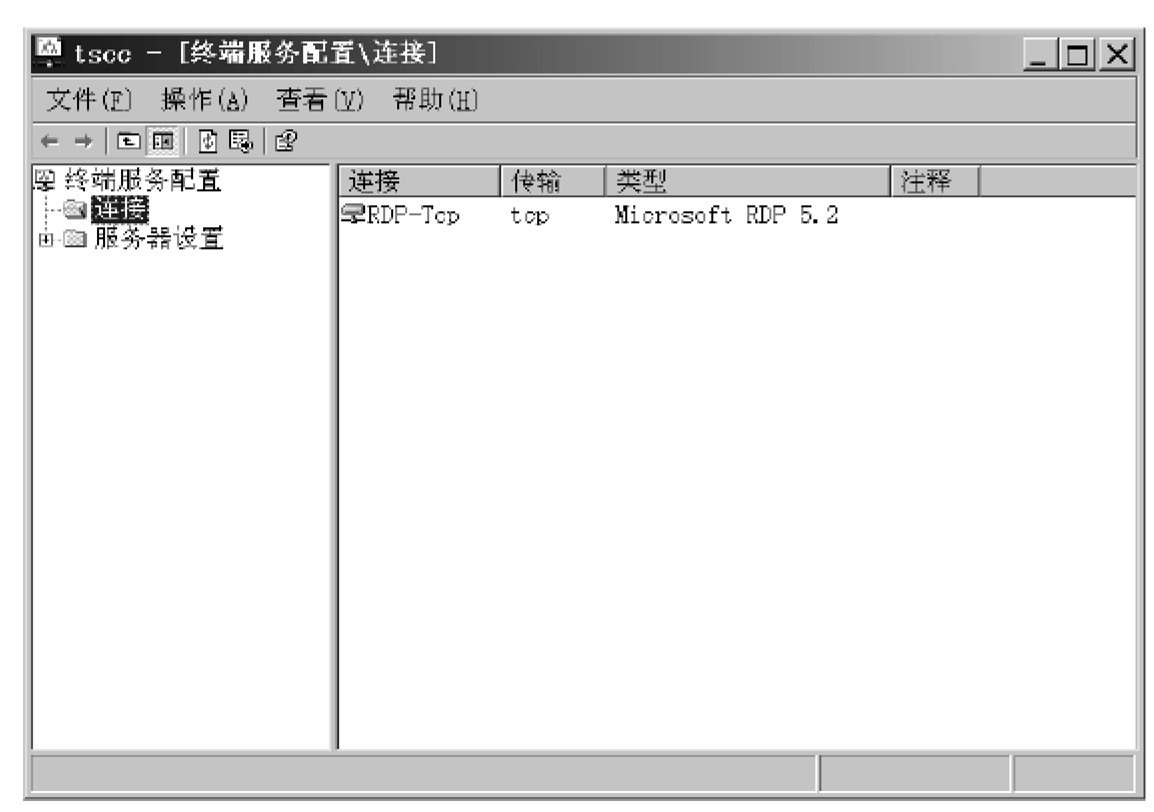




图 4-45　“终端服务配置”窗口　　　　图 4-46　“RDP-Tcp 属性”对话框

（3）单击“高级”按钮，显示所有用户的权限，如图 4-47 所示。

（4）单击“添加”按钮，增加一个新用户，如图 4-48 所示。

（5）选中某一项目单击“编辑”按钮，即可修改某一选定用户的权限。

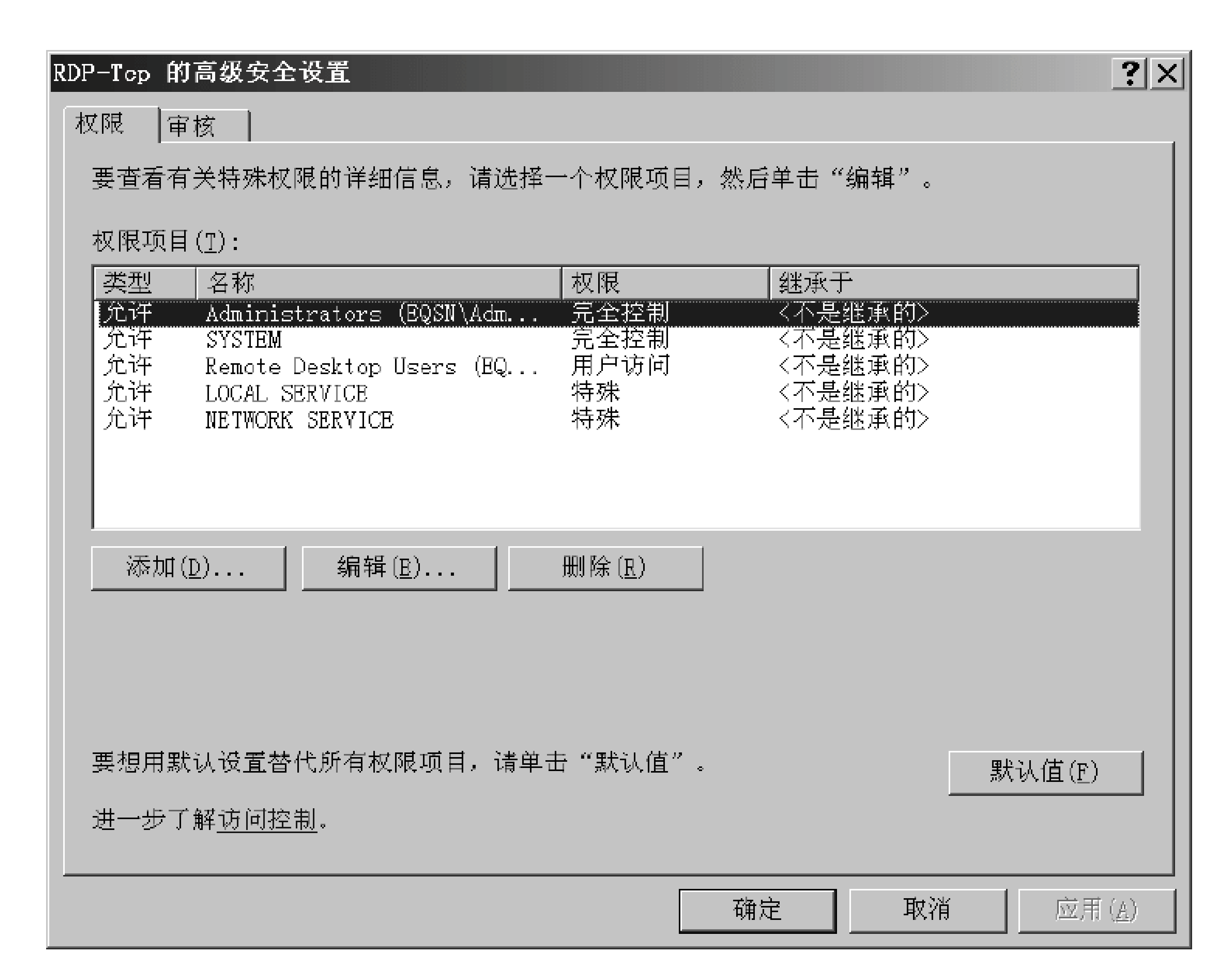


图 4-47 所有用户的权限



图 4-48 修改用户权限

4）终端服务高级设置

（1）更改加密级别

在“RDP-Tcp 属性”对话框中，选择“常规”选项卡，如图 4-49 所示。

在“加密”栏中，单击“加密级别”下拉按钮，其中有 4 种级别：

- 低。使用 56 位密钥，对从客户端传输到服务器的数据进行加密。
- 客户端兼容。使用客户端所支持最大长度的密钥，对从客户端传输到服务器的数据进行加密。

- 高。使用 128 位密钥的强加密算法，对从客户端传输到服务器的数据进行加密。
- 符合 FIPS 标准。使用 Microsoft 加密模块的联邦信息处理标准(FIPS)，对从客户端传输到服务器的数据进行加密。

此外，如果希望此连接进行标准的 Windows 验证，则选中“使用标准 Windows 验证”复选框。

(2) 允许用户自动登录到服务器

在“RDP-Tcp 属性”对话框中，选择“登录设置”选项卡，如图 4-50 所示。

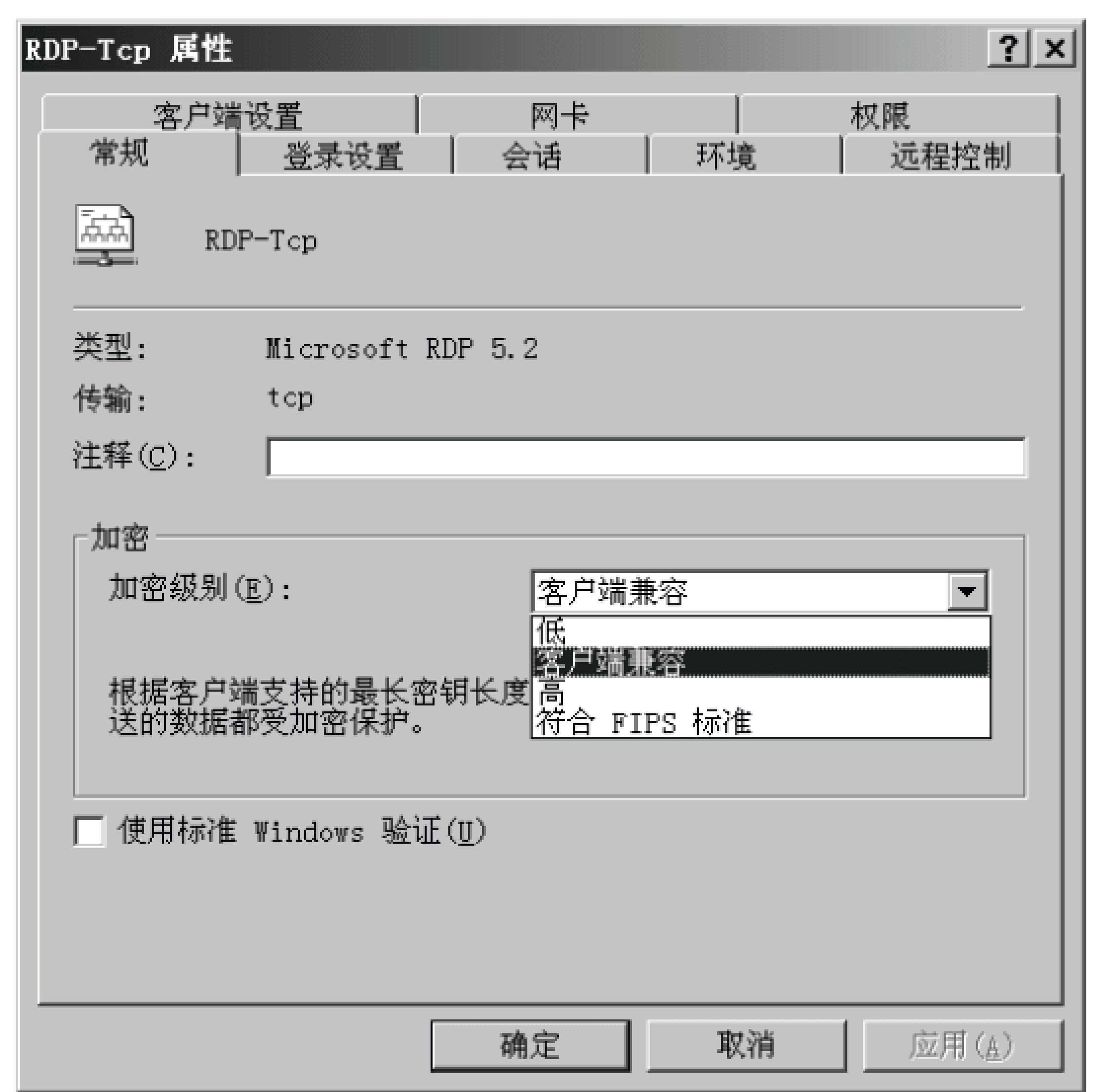


图 4-49 “RDP-Tcp 属性”对话框中的“常规”选项卡



图 4-50 “RDP-Tcp 属性”对话框中的“登录设置”选项卡

默认情况下为“使用客户端提供的登录信息”。

选中“总是使用下列登录信息”单选按钮来设置允许用户登录的信息。“用户名”文本框中填入允许登录到服务器的用户名称；“域”中填入计算机所属域的名称；“密码”和“确认密码”栏中填入该用户登录时所采用的密码。

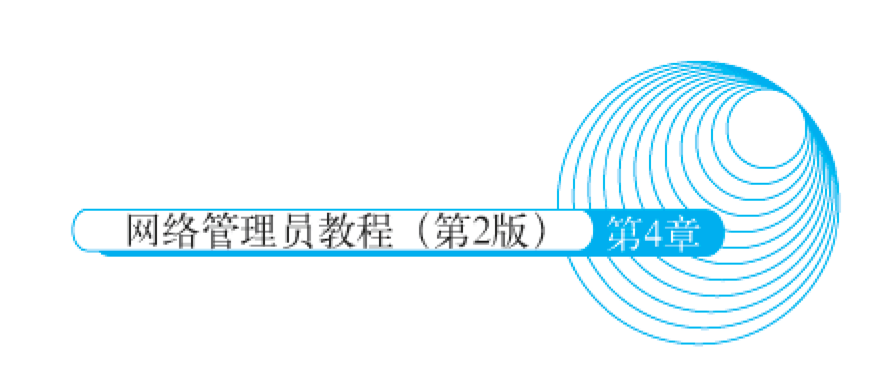
如果要求用户在登录到服务器之前始终被提示输入密码，则选中“总是提示密码”复选框。

(3) 配置终端服务超时和重新连接

在“RDP-Tcp 属性”对话框中，选择“会话”选项卡，如图 4-51 所示。

选中“替代用户设置”复选框，允许用户配置此连接的超时设置。

- 在“结束已断开的会话”下拉列表中，选择断开连接的会话留在服务器上的最长时间。
- 在“活动会话限制”下拉列表中，选择用户的会话在服务器上持续的最长时间。
- 在“空闲会话限制”下拉列表中，选择空闲的会话在服务器上持续的最长时间。



• 选中“替代用户设置”复选框，设置到达会话限制时或者连接被中断时进行的操作。

（4）管理远程控制

在“RDP-Tcp 属性”对话框中，选择“远程控制”选项卡，如图 4-52 所示。

单击“使用具有下列设置的远程控制”单选按钮即可配置该连接的远程控制。

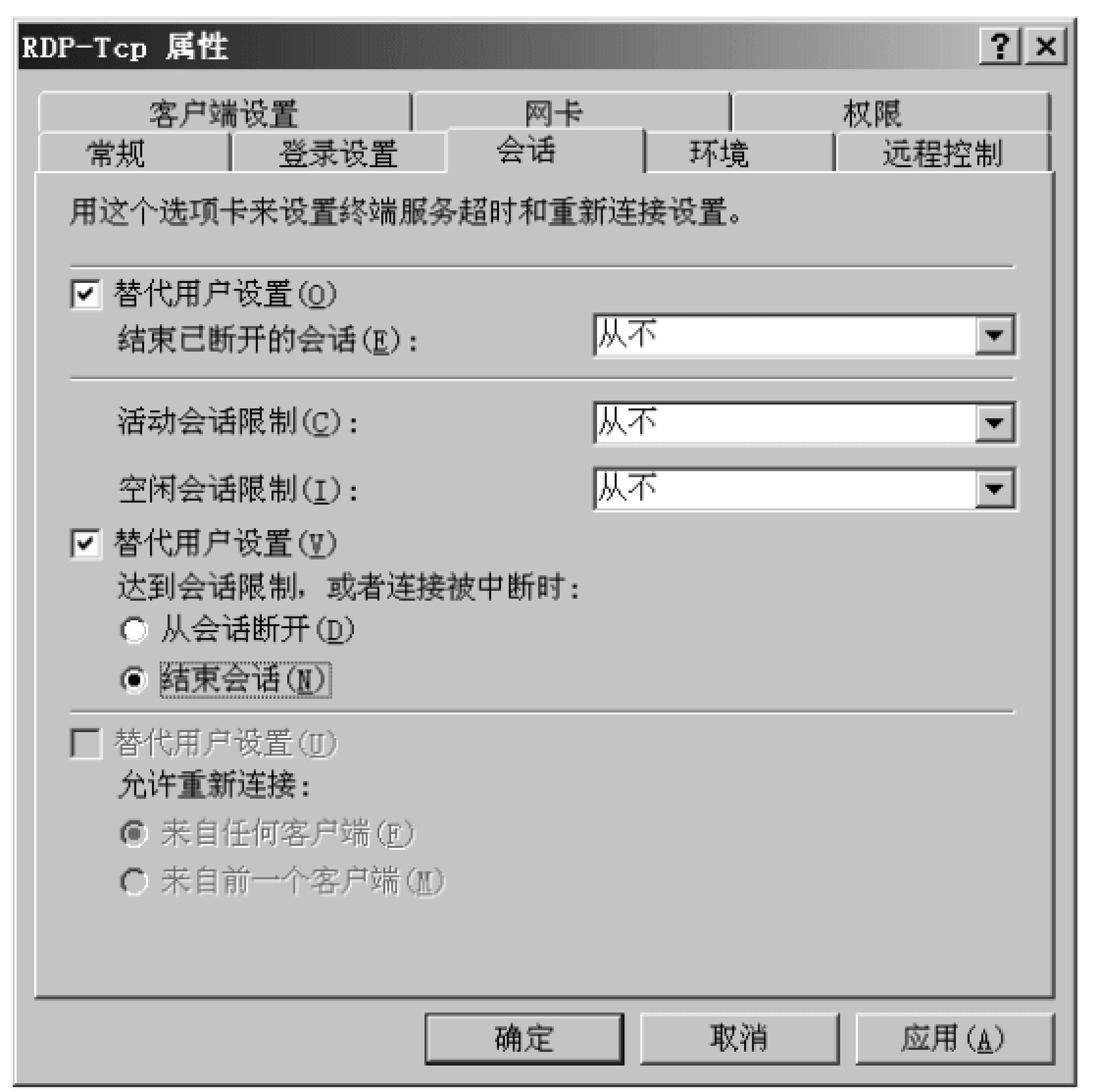


图 4-51 “RDP-Tcp 属性”对话框中的“会话”选项卡

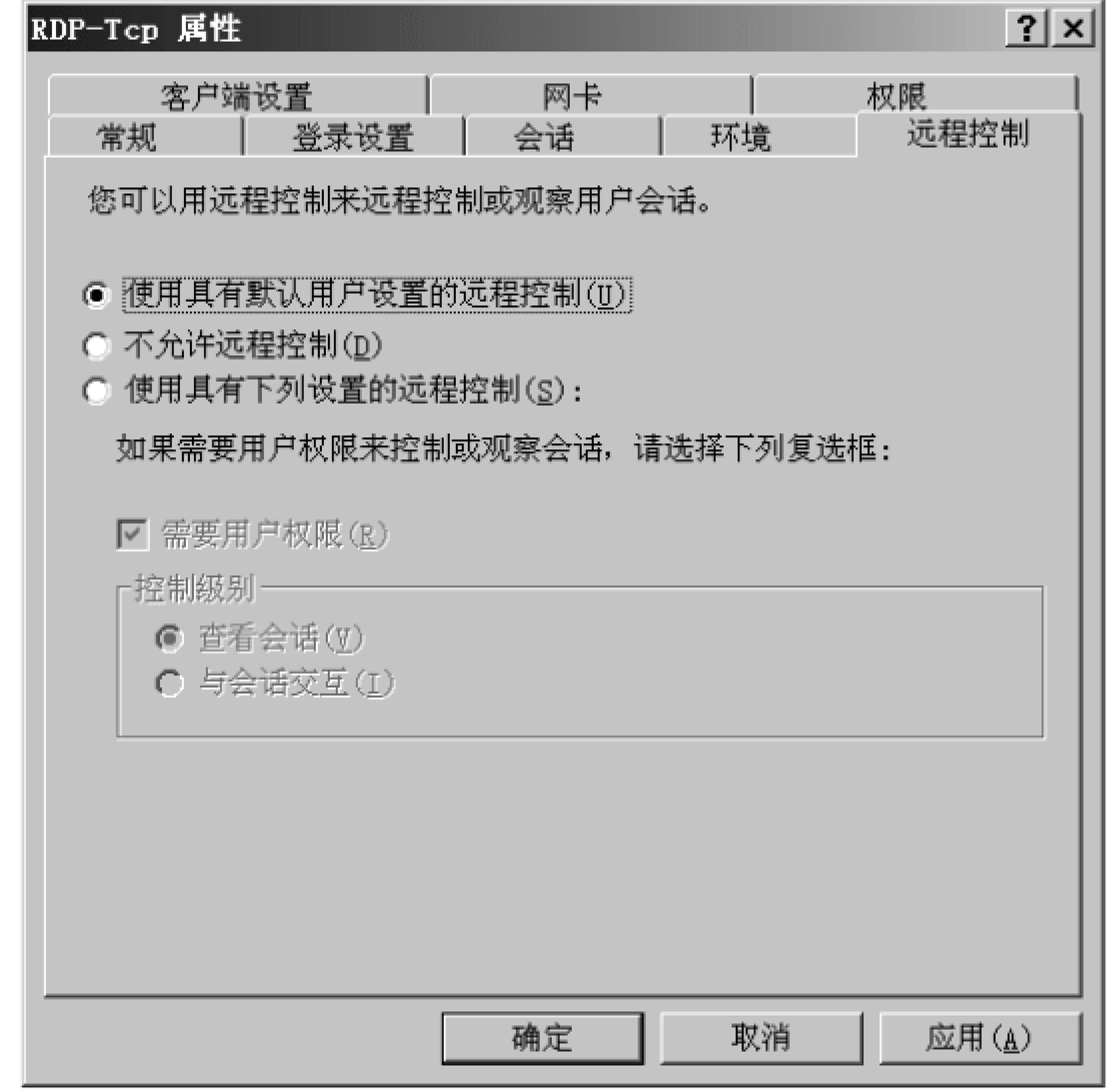


图 4-52 “RDP-Tcp 属性”对话框中的 “远程控制”选项卡

7. 远程管理

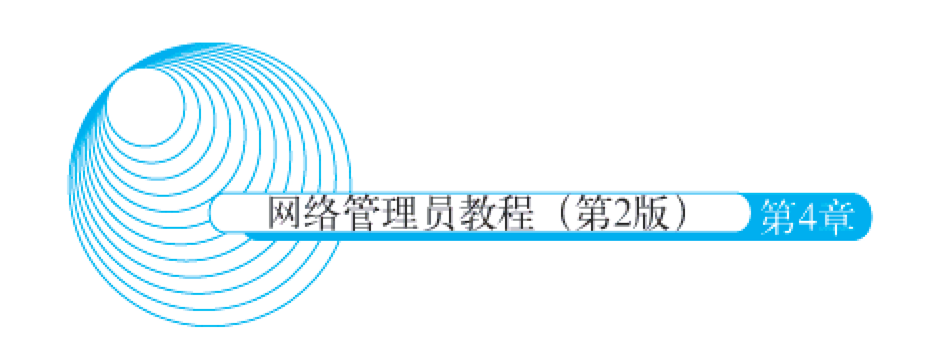
远程管理的使用，与活动目录的使用、组策略的使用一样重要，是衡量 Windows Server 2003 网络管理员、系统管理员水平的重要指标。它既可以是系统中集成的，又可以是由其他单独远程管理软件所提供。在 Windows 系统中，远程管理是集成于其他服务之中，通过使用其他服务或服务组合来实现的。

许多网络设备也引入了“远程管理”理念，如服务器、路由器产品、防火墙和网络打印机等，目的就是方便管理员在不同地方对相应主机或设备进行管理。它与远程控制技术一样，已渗透到各行各业，特别是信息产业的各个领域，应用非常广泛。

随着网络规模的扩大和网络间互联的普及，远程网络管理已作为一种必备手段在各种网络管理系统中广泛应用。Windows Server 2003 作为目前微软最新、功能最强大的网络操作系统，它的远程管理相对 Windows 2000 Server 功能更加强大。

1）Windows Server 2003 远程管理功能改进

（1）“管理远程桌面”功能属于改进型的远程管理功能，它在原来的 Windows 2000 Server 系



统“远程管理”模式中称为“终端服务”。这一远程管理功能可以提供到任何运行 Windows Server 2003 家族操作系统的计算机的桌面的远程访问，并允许从网络中的任一虚拟计算机上管理你的服务器。通过“管理远程桌面”，几乎可以实现从网络上的任何计算机对其他计算机进行管理。“管理远程桌面”基于终端服务技术，是为进行服务器管理而专门设计的。

(2)“远程协助”功能自 Windows XP 系统就开始有了，用户可以使用“远程协助”来邀请受信任的个人与你聊天、观察你的工作屏幕、并在得到你的许可后远程控制你的计算机。也可使用“远程协助”来远程管理计算机。如果你有邀请，则“远程协助”是从运行 Windows XP 或 Windows Server 2003 家族中任何产品的计算机连接到远程计算机的方便途径。连接之后，即可查看远程计算机的屏幕而且可进行实时聊天。如果请求协助的人允许，甚至可以使用鼠标和键盘在远程计算机上进行操作。

(3) 远程管理的 Web 界面(仅限于 Windows Server 2003 Web Edition 版本)

这也是 Windows Server 2003 系统新增的一项远程管理功能。在 Windows Server 2003 Web Edition 上，用于远程管理的 Web 界面是基于超文本标记语言(HTML)的应用程序，用于从远程客户端配置和管理服务器。单个的服务器、整个服务器场和每个服务器的多个站点都可以从单个远程工作站进行管理。

(4)“远程安装服务”(RIS)是从 Windows 2000 系统就开始提供的，但在 Windows Server 2003 家族系统中又对这项远程管理功能进行了一些必要的改进。在这一系统中，对远程安装服务的增强功能包括对 Windows Server 2003 家族和 Windows XP 产品安装的支持；对用于 RIS 安装的应答文件处理有更强的控制；以及对恢复模式下的网络文件的访问。

使用 Windows Server 2003 家族操作系统光盘中包含的工具，可以远程管理运行 Windows 2000 和 Windows Server 2003 家族操作系统的服务器系统；也可以从使用 Windows XP Professional 的计算机远程管理 Windows Server 2003 家族操作系统计算机。

在 Windows Server 2003 家族操作系统中，进行远程管理的方法是多种多样的，主要包括：MMC(微软管理控制台)法、远程桌面连接法、管理远程桌面(终端服务)法、管理工具包法、远程协助法、Telnet 法、远程管理 Web 法和远程存储法等。当然这么多种不同的远程管理方法都有其适用的范围，并不是任何一种方法都适用于所有远程管理领域。

2) Microsoft 管理控制台(MMC)

Microsoft 管理控制台集成了用来管理网络、计算机、服务及其他系统组件的管理工具。可以使用 MMC 创建、保存并打开管理工具单元，这些管理工具用来管理硬件、软件和 Windows 系统的网络组件。MMC 可以运行在各种 Windows 9x/NT 操作系统上，以及 Windows XP Home Edition/XP Professional 和 Windows Server 2003 家族的操作系统上。

MMC 不执行管理功能，但集成管理工具。可以添加到控制台的主要工具类型称为管理单元，其他可添加的项目包括 ActiveX 控件、网页的链接、文件夹、任务板视图和任务。

使用 MMC 有两种方法：在用户模式中使用已有的 MMC 控制台管理系统；在作者模式中，创建新控制台或修改已有的 MMC 控制台。依次有 3 个级别的用户模式，因此共有 4 种默认访问控制台的选项。

若需要在 Windows Server 2003 上，经常对多台计算机进行“远程桌面”管理。用户添加操作如下：

(1) 单击“开始”→“运行”命令，在打开的窗口中输入命令：MMC，如图 4-53 所示。



图 4-53　运行命令

(2) 系统显示 MMC 控制台窗口，如图 4-54 所示。

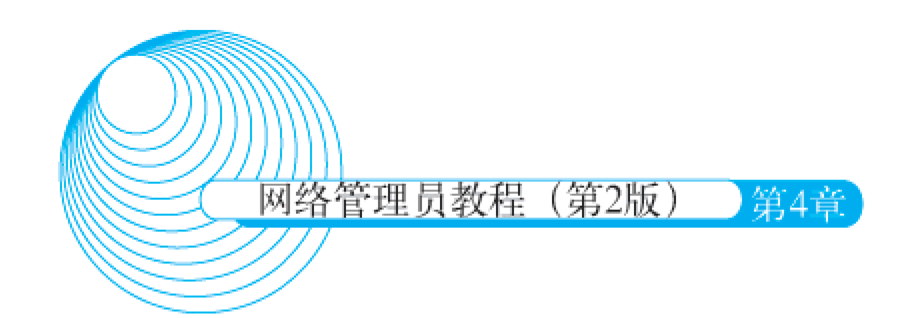


图 4-54　MMC 控制台窗口

(3) 单击“文件”菜单，选择“添加删除管理单元”选项。

(4) 单击“添加”按钮，选择“远程桌面”选项，如图 4-55 所示。

(5) 右击控制台根节点中的“远程桌面”，选择“添加新连接”，在如图 4-56 所示的界面中依次添加目标 IP、名称、用户名、口令、域，完成一个用户的添加。



（6）重复步骤(3)，将目标计算机逐个添加到控制台。



图 4-55 添加远程桌面



图 4-56 添加新连接

3）配置远程桌面连接

“远程桌面连接”是为 Windows Server 2003 系统提供的一种连接远程工作站的远程管理工具，在 Windows XP 系统中以及安装了终端服务器的 Windows 2000 Server 计算机也具有此项功能。其他版本 Windows 系统的计算机不具有此项功能。

（1）在“控制面板”中双击“系统”图标，在“系统属性”对话框中选择“远程”选项卡，在“远程桌面”栏中选中“允许用户远程连接到您的计算机”，如图 4-57 所示。

（2）在“控制面板”中双击“网络连接”图标，右击“本地连接”图标，选择“属性”选项，在打开的对话框中选择“高级”选项卡，如图 4-58 所示。

（3）在“Internet 连接防火墙”栏中取消选择“通过限制或阻止来自 Internet 的对此计算机的访问来保护我的网络”复选框。

（4）单击“确定”按钮允许远程访问。

4）使用“远程桌面连接”

（1）“远程桌面连接”工具在“开始”→“所有程序”→“附件”→“通讯”路径下，可直接单击打开。随即弹出一个对话框，要求输入要远程连接的计算机名或 IP 地址，如图 6-59 所示。

（2）单击“选项”按钮，即可弹出一个可以对该项远程连接详细配置的对话框，如图 4-60 所示。在这个对话框中包括 5 个选项卡，可以进行非常全面的连接配置，具体操作在此不再详细介绍。

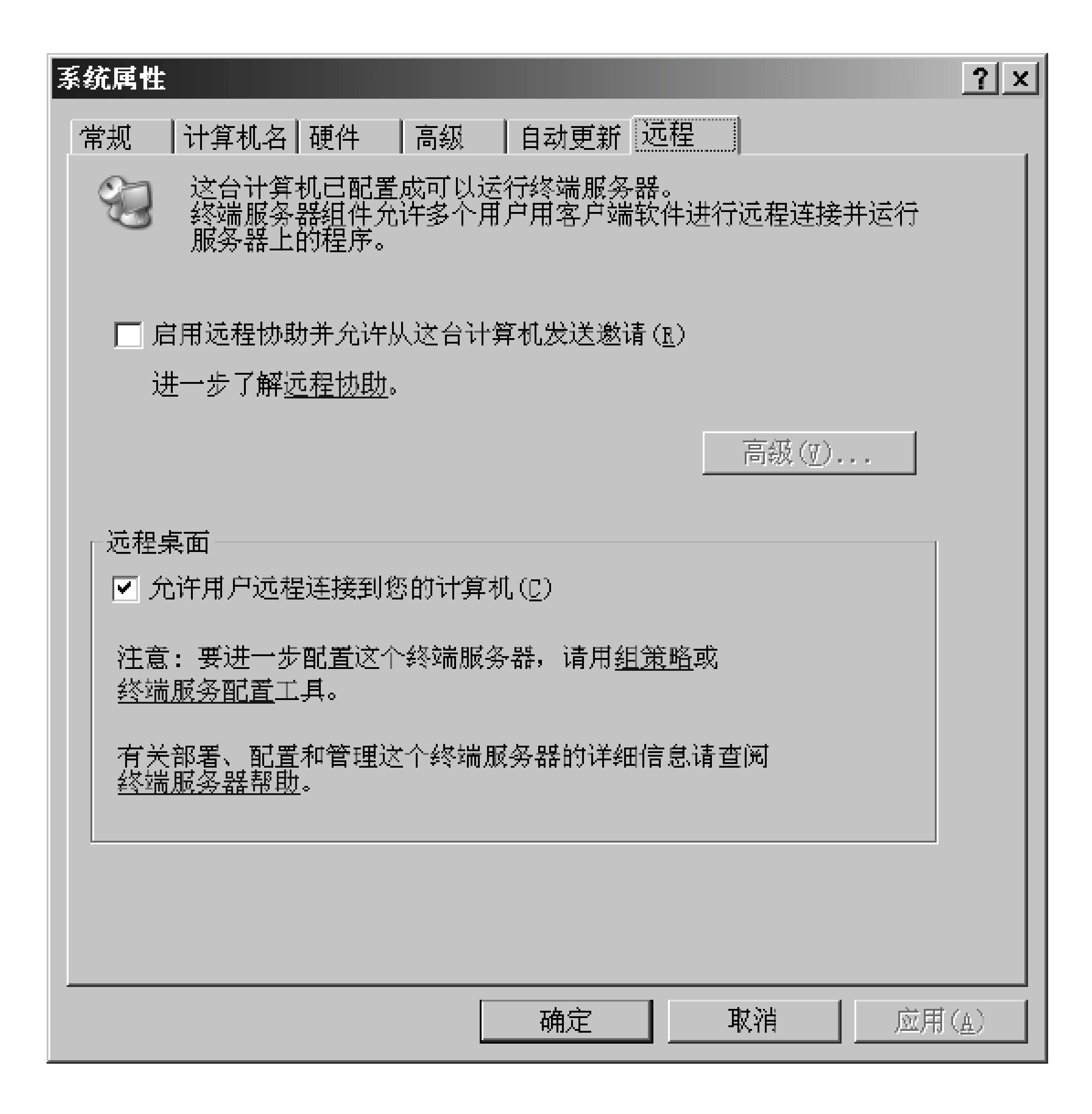


图 4-57 “系统属性”对话框中的“远程”选项卡

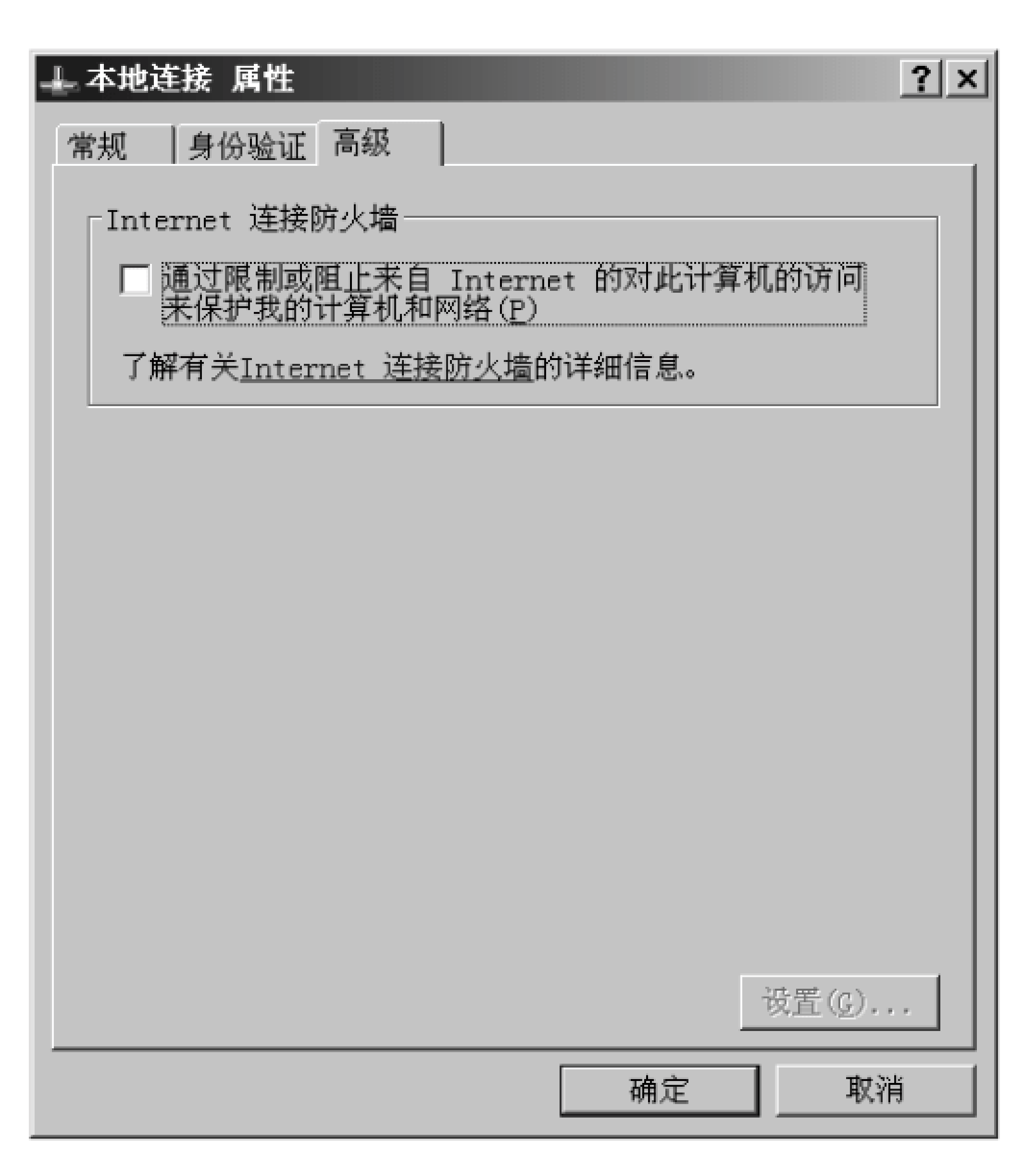


图 4-58 本地连接属性



图 6-59 “远程桌面连接”对话框



图 4-60 “远程桌面连接”对话框

（3）使用“远程桌面连接”，可以很容易地连接到终端服务器或其他运行远程桌面的计算机，所需要的仅是网络访问和连接到其他计算机的权限。可以随意地为连接指定特殊设置，并保存

设置以用于下次连接,远程连接如图 4-61 所示。

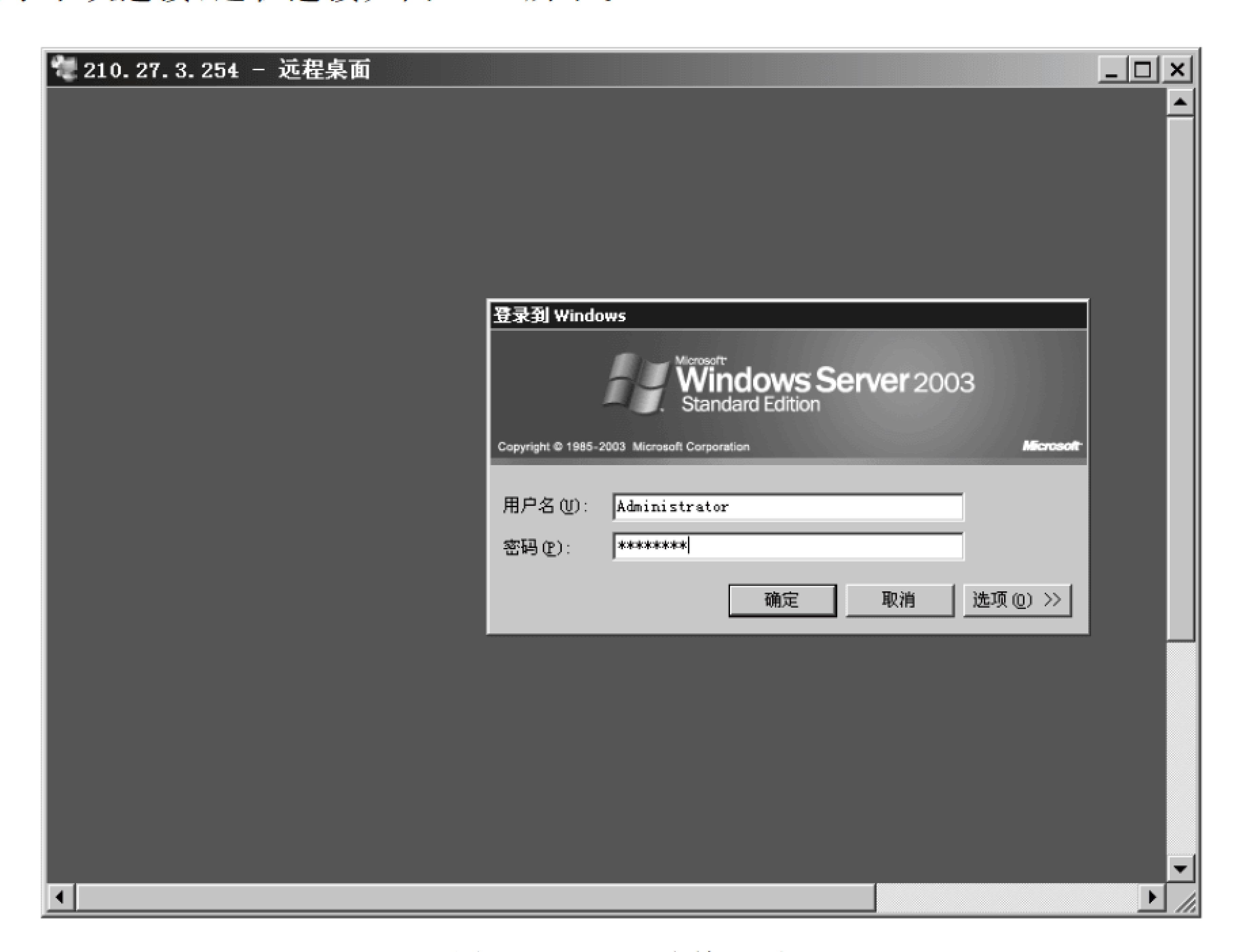


图 4-61　远程连接登录

要使计算机可接受远程连接,远程计算机必须运行 Windows NT4 Terminal Server Edition、Windows 2000 Server、Windows XP Professional 或 Windows Server 2003 操作系统。

5）远程桌面连接的远程管理

通过远程桌面连接方式可进行的远程管理操作如下:

（1）在远程会话中进行剪切和粘贴操作。很多"远程桌面和终端服务器"连接提供剪贴板共享,可从"远程桌面"会话运行的程序中进行剪切并粘贴到本地计算机上运行的程序。当从某个程序剪切或复制信息时,该信息会被移动到剪贴板并保留在那里,直到清除剪贴板或者剪切或复制了另一片信息。"剪贴板查看器"中的剪贴板窗口将显示剪贴板中的内容。可以随时将剪贴板中的信息粘贴到任何文档。但是,信息仅暂时存储在剪贴板上。

共享剪贴板使其内容与本地剪贴板同步。可从"远程桌面连接"窗口内的文档中复制和粘贴文本或图形,然后将其粘贴到本地计算机上的文档。

（2）使终端服务器使用本地资源。根据网络上组策略的不同设置,可以选择是否允许终端服务器访问本地计算机上的磁盘驱动器、串行口、打印机或智能卡,这称为"资源重定向"。除非组策略设置禁止资源重定向,否则可以将本地资源重定向到终端服务器。方法是在"远程桌面连接"对话框的"本地资源"选项卡的"本地设备"栏中选中相应的可重定向本地设备项,如

图 4-62 所示。

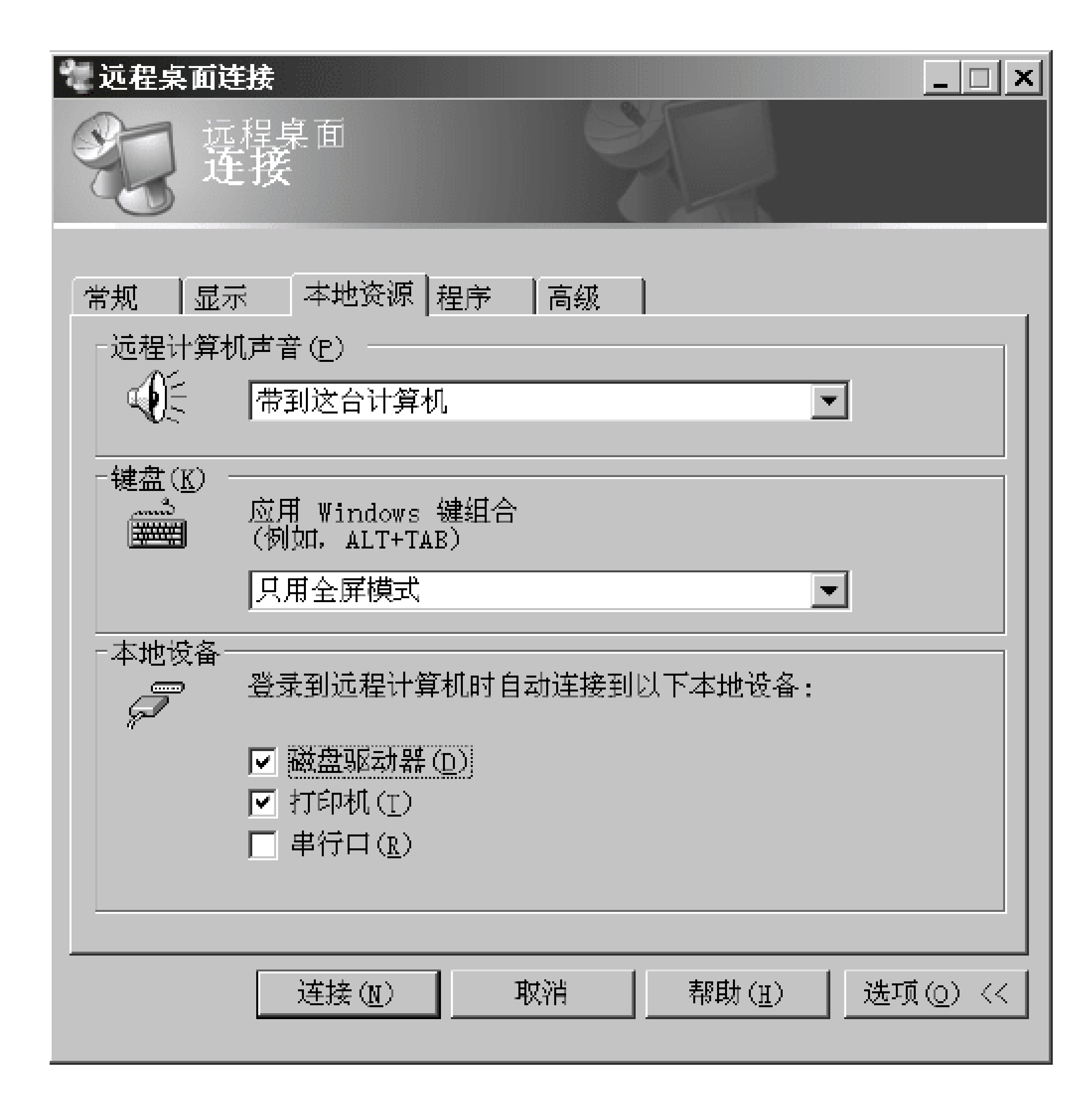


图 4-62　可重向本地设备

使这些资源对终端服务器可用，意味着终端服务器可在会话期间使用这些资源。例如，假定选择使本地磁盘驱动器对终端服务器可用。尽管这使得将文件复制到终端服务器或从终端服务器复制文件都非常容易，但这也意味着终端服务器可以访问本地磁盘驱动器的内容。在这种情况不适当的时候，可取消选中相应复选框，以使本地磁盘驱动器或其他任何本地资源不会被重定向到终端服务器。默认情况下，磁盘驱动器、串行口以及智能卡的资源重定向为关闭。

(3) 在远程会话中访问本地文件和文件夹。可配置“远程桌面连接”，选择如图 4-62 所示对话框中的“磁盘驱动器”复选项，使本地驱动器在连接到远程计算机时可用。

在“远程桌面连接”会话中，本地驱动器将按以下指派方式出现在 Windows 资源管理器中：＜computername＞ 上的 ＜driveletter＞。在图 4-63 中 computername 为 LEI，driveletter 为 C。

(4) 从远程会话打印到本地打印机。打印机重定向将打印作业从终端服务器或“远程桌面”计算机路由到本地计算机(也称为“客户端计算机”)连接的打印机。有“自动”和“手动”打印机重定向两种方法可提供对本地打印机的访问。当在远程计算机上运行的 Windows 版本中没有本地打印机所需要的驱动程序时，使用手动重定向。具体操作在此不再赘述。

(5) 使用终端服务快捷键。如果在如图 4-62 所示对话框的“键盘”栏中的“应用 Windows 组合键”下拉列表中选择“本地计算机上”选项时，则可使用终端服务快捷键执行许多相同的功能。这些快捷键及各自的作用如表 4-3 所示。

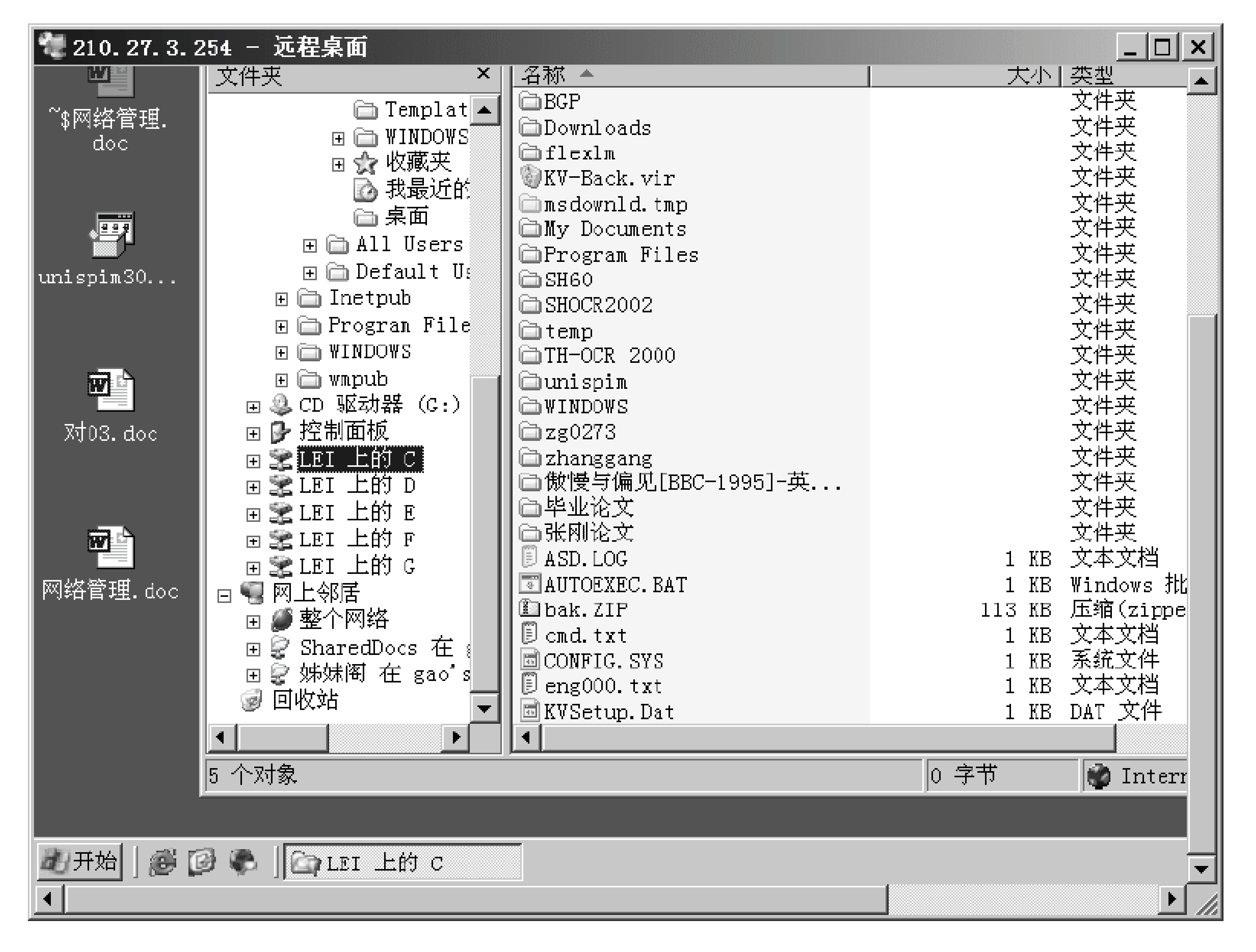


图 4-63 驱动器指派方式

表 4-3 终端服务快捷键及说明

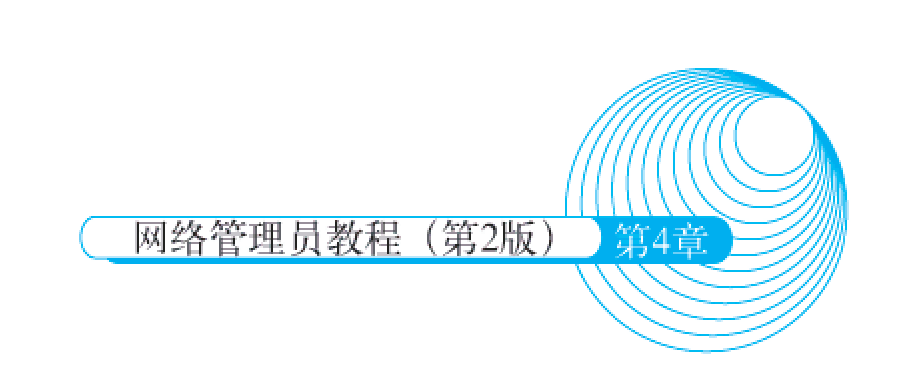
快捷键	说明
Alt+Page Up	从左到右切换程序
Alt+Page Down	从右到左切换程序
Alt+Page Insert	按照程序的启动顺序来切换程序
Alt+Page Home	显示“开始”菜单
Ctrl+Alt+Break	在窗口和全屏之间切换客户端

即使选择“远程计算机上”选项，来应用 Windows 键组合时，Ctrl+Alt+Break 和 Ctrl+Alt+End 也都在所有“远程桌面连接”会话中可用。

4.2.4 配置 IIS 服务

1. IIS 服务器的基本概念

在组建局域网时，可以利用因特网信息服务器（IIS，Internet Information Server）来构建 WWW 服务器、FTP 服务器和 SMTP 服务器等。IIS 服务将 HTTP 协议、FTP 协议与 Windows Server 2000 出色的管理和安全特性结合起来，提供了一个功能非常全面的软件包，面向不同的



应用领域给出了 Internet/intranet 服务器解决方案。在 Windows 2000 Server 中集成了 IIS 5.0 提供的更为方便的安装/管理功能和增强的应用环境，基于标准的分布协议，改进的性能表现和扩展性，以及更好的稳定性和易用性。

1）WWW 服务

WWW 即 World Wide Web，是图形最为丰富的 Internet 服务。Web 具有很强的链接能力，支持协作和工作流程，可以给世界各地的用户提供商业应用程序。Web 是 Internet 上主机的集合，使用 HTTP 协议提供服务。基于 Web 的信息使用超文本置标语言，以 HTML 格式传送，它不但可以传送文本信息，还可以传送图形、图像、动画、声音和视频信息。这些特点使得 WWW 成为遍布世界的信息交流的平台。

2）FTP 服务

文件传输协议（FTP，File Transfer Protocol）是在 Internet 中两个远程计算机之间传送文件的协议。该协议允许用户使用 FTP 命令对远程计算机中的文件系统进行操作。通过 FTP 可以传送任意类型、任意大小的文件。在 Windows Server 2003 中 IIS 6.0 里内置了 FTP 模块。

3）SMTP 服务

简单邮件传输协议（SMTP，Simple Mail Transfer Protocol）在客户机应用程序和远程计算机的邮件服务器之间传送邮件信息。也可以通过配置域控制器，使之利用 SMTP 服务跨越站点上的链接实现邮件复制功能。

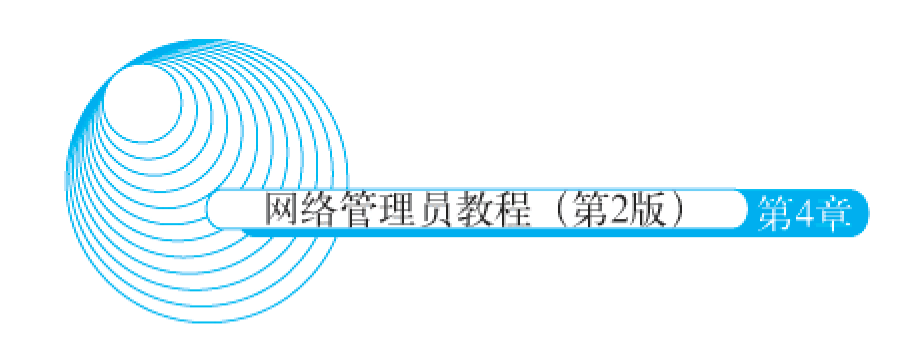
4）POP3 服务

邮局协议（POP，Post Office Protocol）第 3 版是目前使用最广泛的邮件服务。POP3 的功能是邮件的存储和管理，能为用户提供账号、密码和身份验证功能，与 SMTP 服务配合，提供完整的邮件服务。

2. 安装 IIS 服务

不同的 Windows 系统内置的 IIS 版本是各不相同的，Windows Server 2003 为 IIS 6.0，默认状态下没有安装 IIS 服务，必须手工安装。IIS 是微软出品的架设 Web、FTP、SMTP 服务器的一套整合软件，安装 IIS 服务需要加载以下模块。

- Frontpage 服务器扩展：使用 Microsoft FrontPage 和 Visual InterDev 来建立和管理站点。
- Internet 服务器管理：IIS 的管理界面。此界面在 Microsoft 管理控制台（MMC）中以管理单元显示。
- Prosonal Web Manage：个人 Web 管理，这是一个图形管理界面。
- SMTP Service：简单邮件传输协议服务。
- World Wide Web 服务器：World Wide Web 服务器支持 Web 站点的访问。
- 公用文件：所需要的 IIS 程序文件，包括出版物、站点内容，以及 Web 和 FTP 服务器管理



标题。

- FTP 服务器：支持文件传输协议，允许建立 FTP 站点，用于上传和下载文件。

具体安装步骤如下：

（1）IIS 的安装过程非常简单。依次单击“开始”→“控制面板”→“添加/删除程序”命令。单击“添加/删除 Windows 组件”按钮，启动“Windows 组件向导”。

（2）在“组件”列表中，选中“应用程序服务器”复选框，单击“详细信息”按钮，如图 4-64 所示。

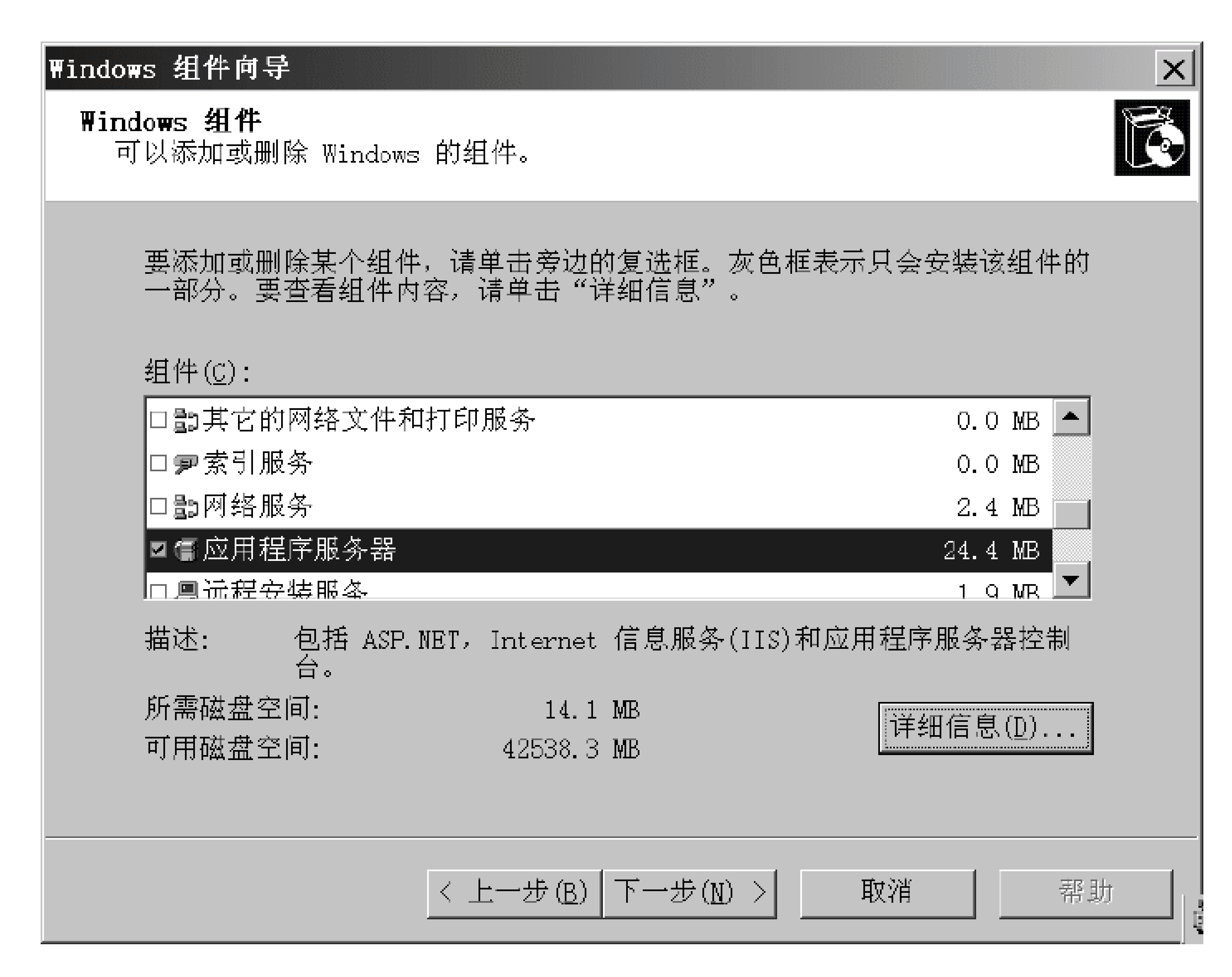


图 4-64 安装 IIS 服务（一）

（3）在“应用程序服务器”对话框中，选中“Internet 信息服务（IIS）”，单击“详细信息”按钮，在“Internet 信息服务（IIS）的子组件”列表中勾选想要添加的服务，比如 SMTPService、文件传输协议（FTP）服务，如图 4-65 所示。

（4）单击“确定”按钮返回 Windows 组件向导，再单击“下一步”按钮，按照系统提示插入光盘，完成安装。

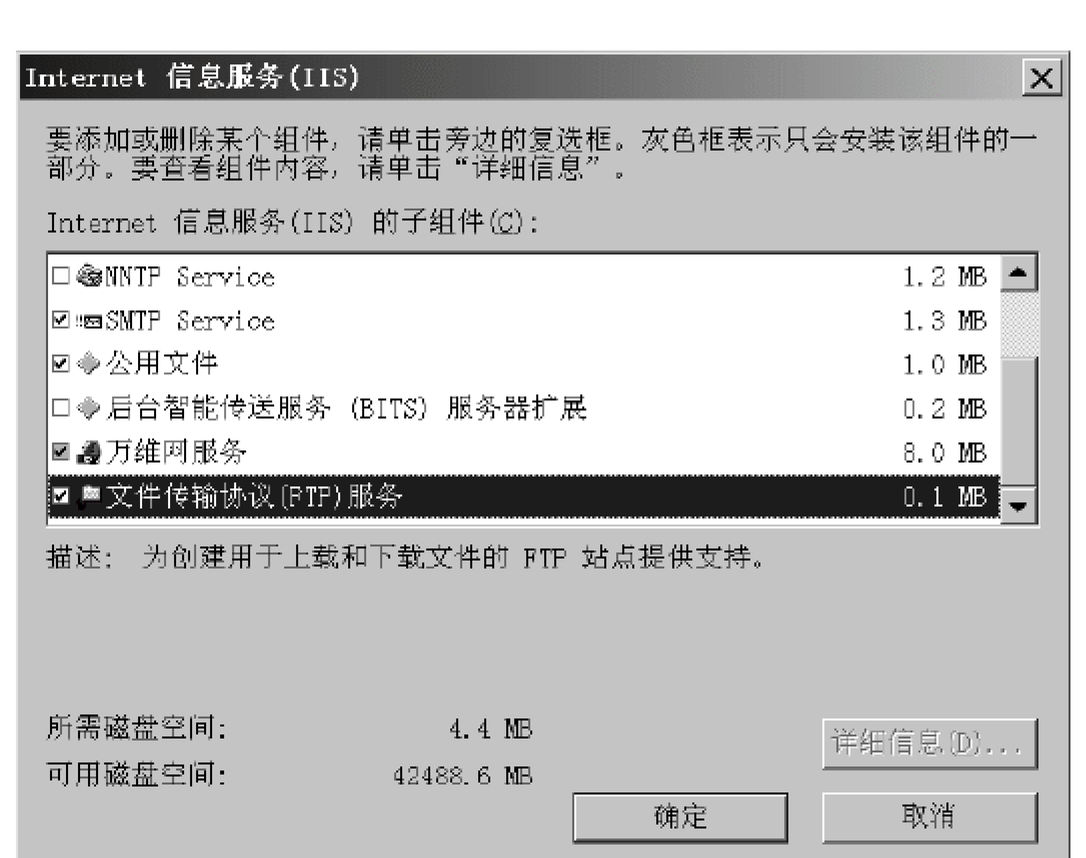
3. 配置 Web 服务器

1）基本配置

创建 Web 服务器可以通过修改 IIS 默认的 Web 站点实现。在控制面板中选择“管理工具”，然后在弹出的窗口中选择“Internet 信息服务（IIS）管理器”，打开 IIS 主界面，在“默认网站”的快捷菜单中选择“属性”进入“默认网站 属性”窗口。

在“网站”选项卡上的“描述”里可以为网站取一个标识名称，如果本机分配了多个 IP 地址，则要在 IP 地址框中选择一个赋予此 Web 站点的 IP 地址，如图 4-66 所示。其中：

- 网站标识：在“描述”栏填写网站的名称。
- IP 地址：为了安全起见，通常要为 Web 站点分配一个 IP 地址，在该下拉列表中，选中与局域网连接的网卡的 IP 地址。
- TCP 端口：由于 HTTP 协议使用 80 号端口，所以在这一栏输入“80”。



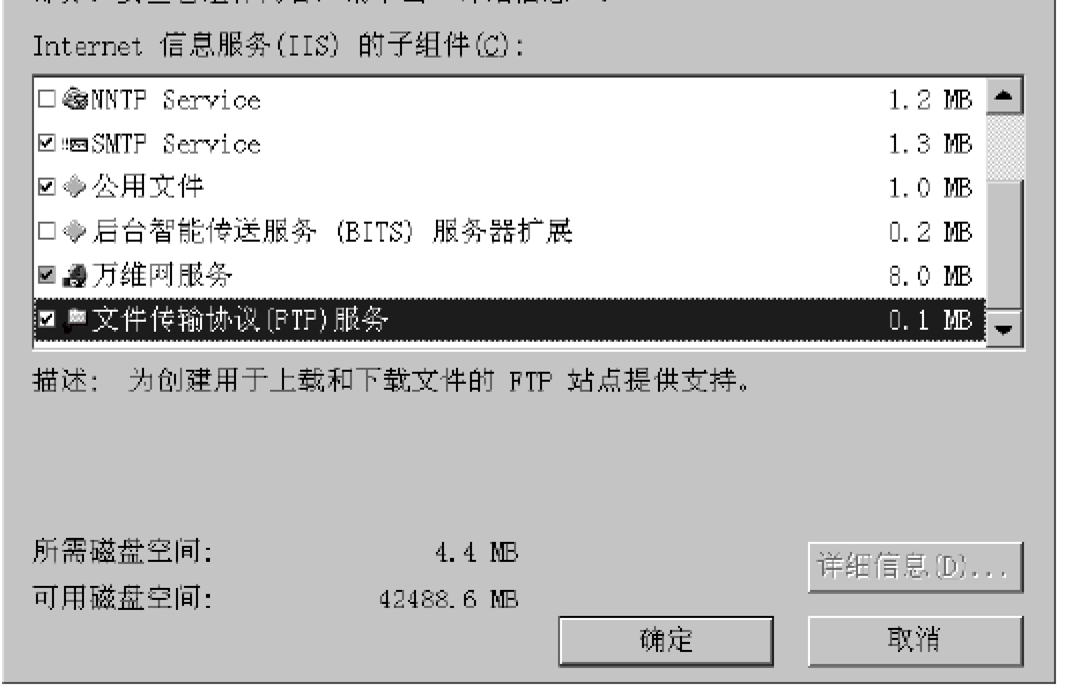


图 4-65　安装 IIS 服务(二)

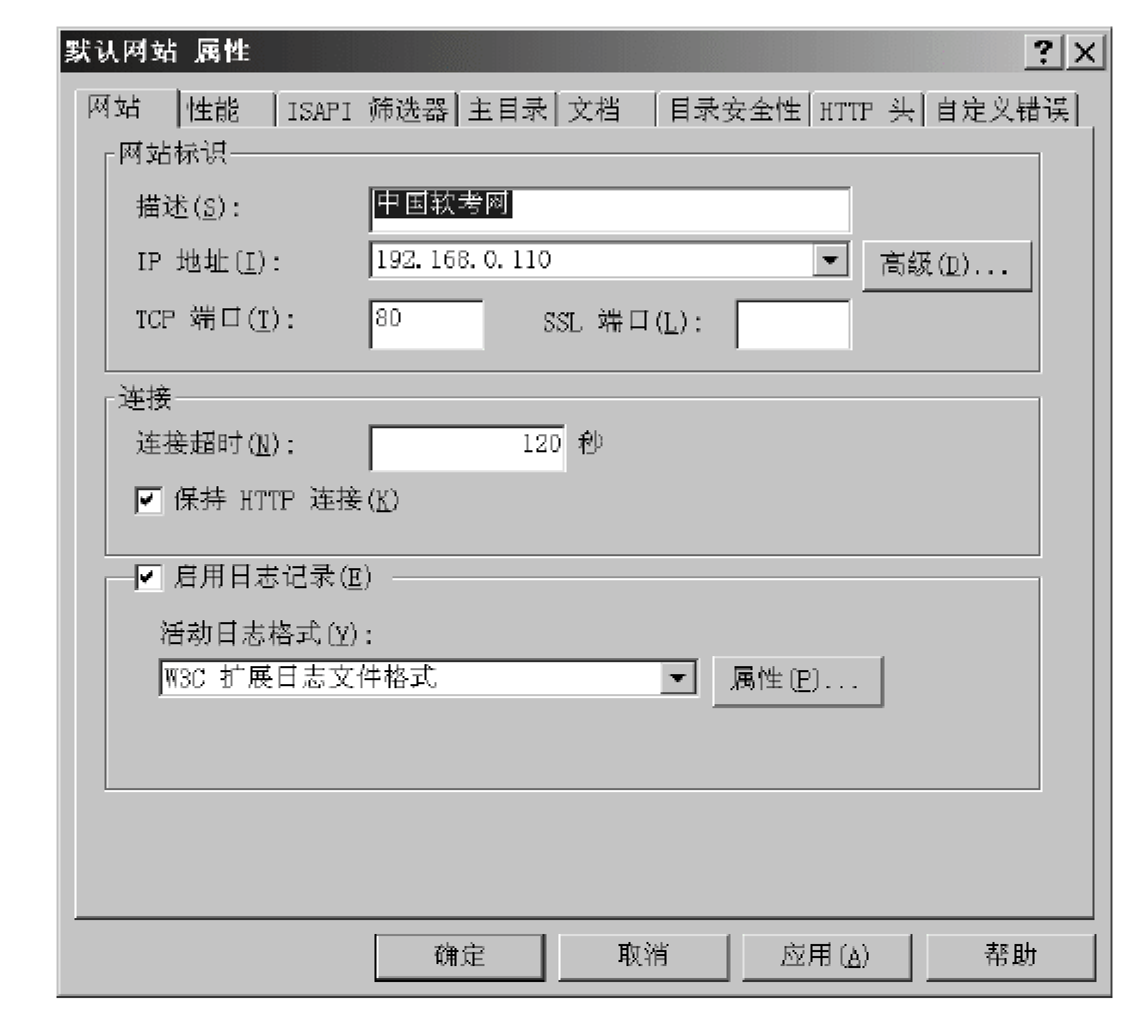


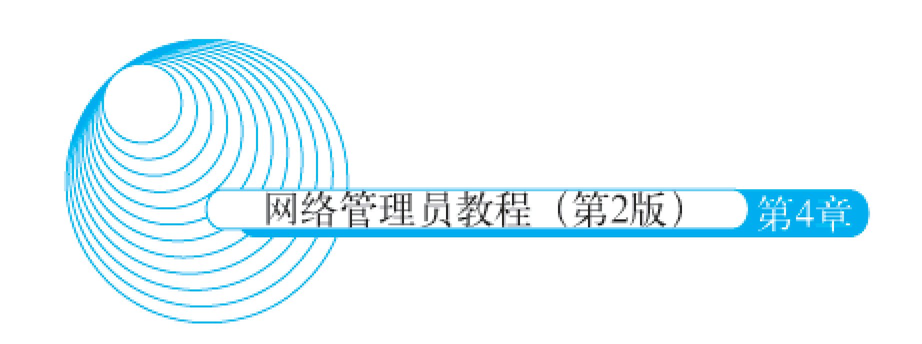
图 4-66　配置 Web 服务器(一)

在“主目录”选项卡中指定网站 Web 内容的来源。主目录是存放网站文件的文件夹，在这个主目录下还可以任意创建子目录。通常 Web 服务器的主目录都位于本地磁盘系统中，所以选择“此计算机上的目录”。如果网站要建立在联网的其他计算机上，则选择“另一台计算机上的共享”。如果要在互联网的某台服务器上建立网站，则选择“重定向到 URL”，如图 4-67 所示。

下面对几个概念给予解释：

- 访问权限：在“默认站点 属性”中选择“主目录”选项卡，可以设置主目录的访问权限。由于网站主要是供用户浏览的，所以只要选择“读取”即可。“写入”权限是供管理员使用的。如果还要为用户提供目录浏览权限，则必须选取“目录浏览”选项。
- 日志访问：在日志文件中记录对目录的访问。
- 脚本资源访问：允许用户访问程序中的脚本资源。
- 目录浏览：允许用户浏览目录中的文本列表。

在“默认站点 属性”对话框中单击“文档”选项卡，可以看到几个默认的主页文件 Default.htm、Dfault.asp、index.htm 和 iisstart.htm，可以修改其中的任何一个文档来建立自己的网站，



如图 4-68 所示。

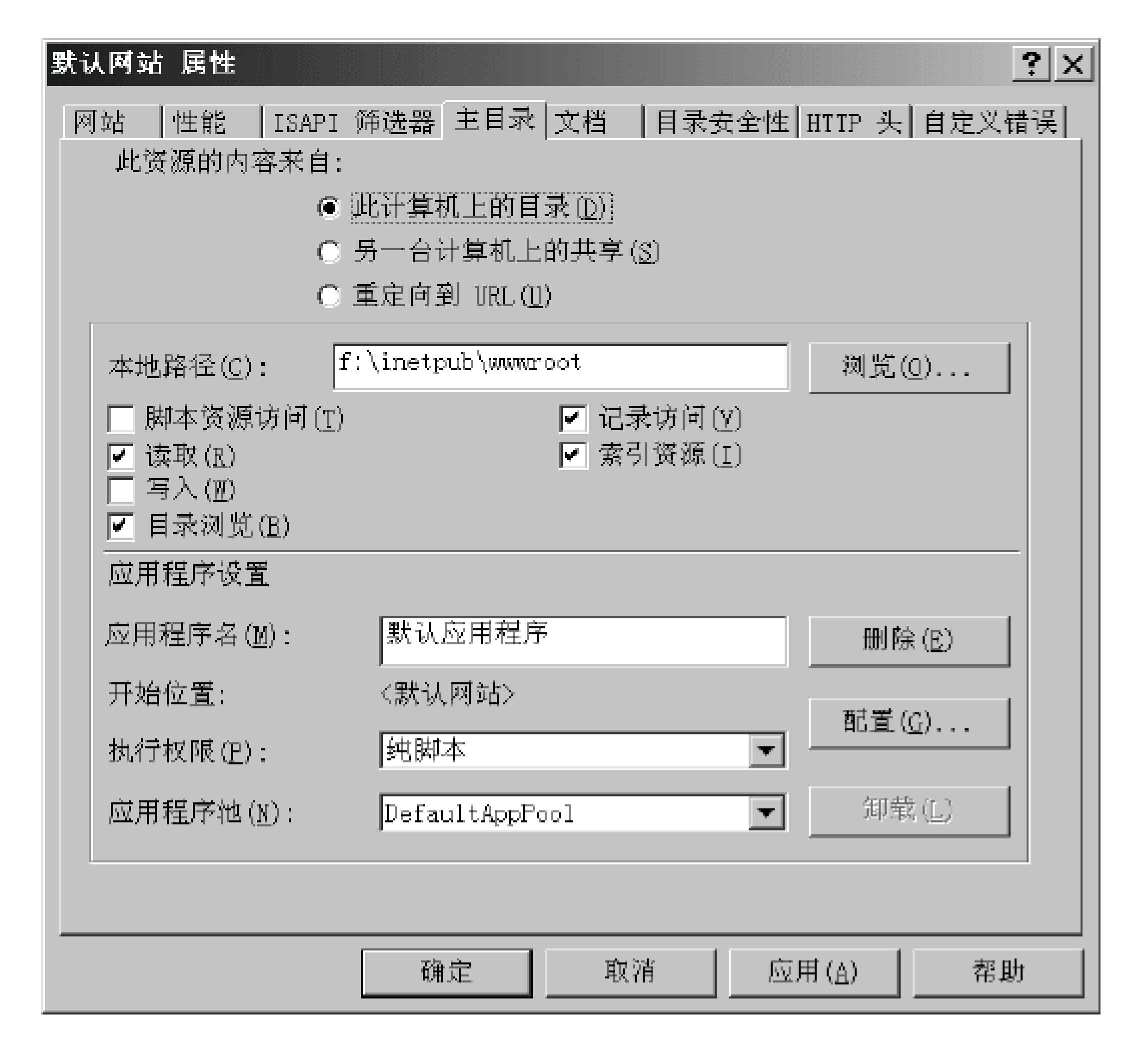


图 4-67　配置 Web 服务器(二)



图 4-68　配置 Web 服务器(三)

Web 站点的配置是通过图形用户界面来进行的,可以根据提示练习配置网站的过程。

2）安全配置

为了保证 Web 网站和服务器的运行安全,可以在“目录安全性”选项卡上为网站进行身份验证和访问控制、IP 地址和域名限制的设置,如果没有别的要求一般采用默认设置,如图 4-69 所示。

网站的匿名访问关系到网站的安全问题。可以编辑“匿名访问和身份验证控制”来设置匿名访问的用户账号。系统中默认的用户权限比较低,只具有基本的访问权限,比较适合匿名访问。为了便于用户匿名访问,要选取“启用匿名访问”复选框,这样不必输入账号和密码就可访问网站,如图 4-70 所示。

对于具有特殊权限、不允许匿名访问的用户要设置身份验证方案。这里有两种身份验证方案:

(1）基本身份验证。采用这种身份验证方法进行登录的过程如下:

① Web 浏览器显示一个对话框,用户输入为其分配的用户名和密码(凭据);

② 浏览器试图根据用户输入的凭据与服务器建立连接,明文密码在进入网络前要经过 Base64 编码;

③ 如果用户的凭据被拒绝,浏览器将重新显示身份验证窗口,用户在连接失败前可以进行 3 次尝试登录;如果用户的凭据有效,则登录成功,连接建立。



图 4-69　创建 Web 服务器(四)

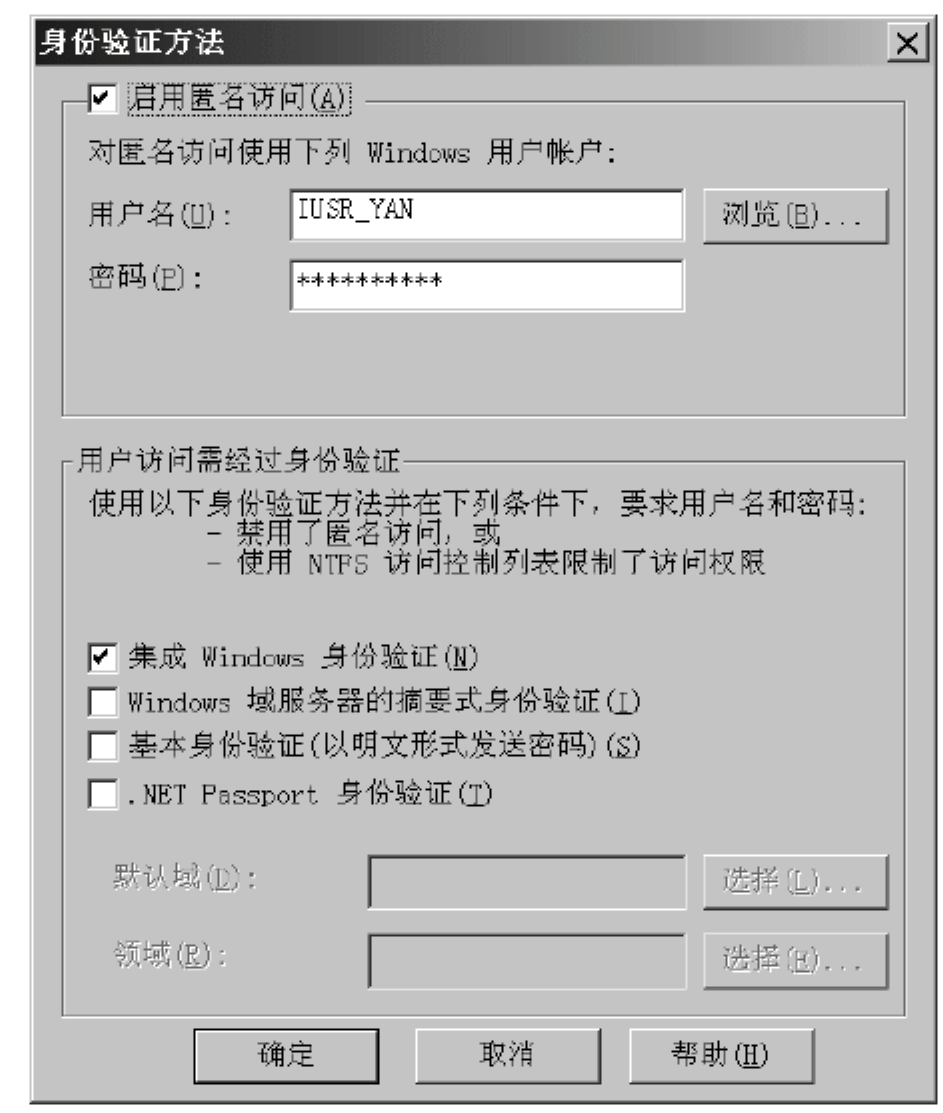


图 4-70　创建 Web 服务器(五)

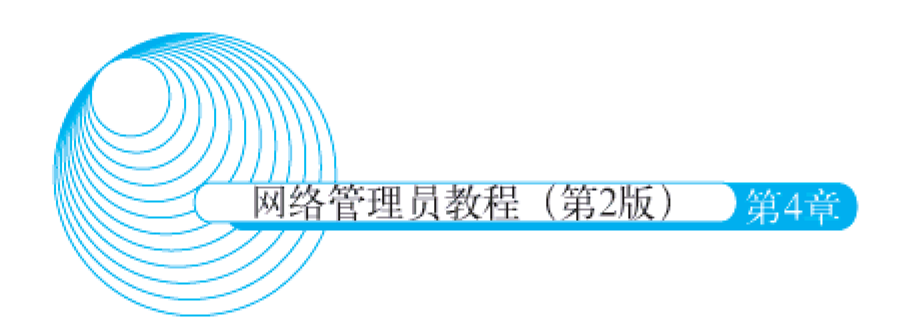
(2) 集成 Windows 身份验证。在这种身份验证方式中，用户名和密码在发送前要经过加密处理，所以是一种安全的身份验证方案。这种身份验证方案结合了 Windows NT 质询/响应身份验证(NTLM)和 Kerberos v5 身份验证两种方式。Kerberos v5 是 Windows 2000 分布式服务架构的重要功能，为了进行 Kerberos v5 身份验证，客户端和服务器都必须与密钥发行中心(KDC)建立可信任的连接。如果用户系统在域控制器中安装了 Active Directory 服务，而且浏览器支持 Kerberos v5 身份认证协议，则使用 Kerberos v5 身份验证，否则使用 NTLM 身份验证。集成 Windows 身份验证的过程如下：

① 在这种认证方式下，用户不必输入凭据，而是使用客户端计算机上当前的 Windows 用户信息作为输入的凭据；

② 如果最初的信息交换未能识别用户的合法身份，则浏览器将提示用户输入账号名和密码，直到用户输入了有效的账号名和密码，或者关闭了对话提示框。

集成 Windows 身份验证方案虽然比较安全，但是通过代理服务器建立连接时这个方案就行不通了。所以集成 Windows 身份验证最适合于 intranet 环境，这样用户和 Web 服务器都在同一个域内，而且管理员可以保证每个用户浏览器都在 IE 2.0 版本以上，保证支持这种身份验证方案。

在目录安全性选项卡中还有一项是“IP 地址及域名限制”，可以编辑这个选项，对访问站点的计算机进行限制。在弹出的“IP 地址及域名限制”对话框中可以采用“授权访问”或“拒绝访问”来排除/允许某些计算机的访问权限。



在“目录安全性”选项卡中最后一个选项是“安全通信”，在这里可以通过“服务器证书”按钮打开“Web 服务器证书向导”创建一个新证书，在填写适当的内容后，建立的新证书要经过证书颁发机构的公正，然后再一次用“Web 服务器证书向导”把证书颁发机构发来的证书文件附加到自己创建的证书上去。

4.3 Red Flag Server 4.0

4.3.1 红旗 Linux 简介

随着 Linux 的快速发展，国家在电子政务技术标准中明确表示，今后电子政务将首选国产化软件，而 Linux 作为优秀的开放源代码操作系统，无论从安全性还是低成本都有利于中国软件民族产业化的发展，Linux 在中国电子政务中的应用似乎开始逐步形成固化。在北京电子政务、广东省电子政务中都率先采用了 Linux 操作平台。

需要指出的是，世界上只有一个 Linux，而不同厂商推出的只是具有不同特色的发行版本，目前国内主要的 Linux 发布商如表 4-4 所示。

表 4-4 国内主要的 Linux 发布商

国内 Linux 发布商	产品名称（英文）	产品名称（中文）
北京中科红旗软件技术有限公司	Red Flag Linux	红旗 Linux
中国计算机软件与技术服务总公司	COSIX Linux	中软 Linux
Xteam（中国）软件技术有限公司	Xteam Linux	冲浪 Linux
蓝点软件技术有限公司	Blue Point Linux	蓝点 Linux
联想集团（联想电脑公司）	Happy Linux	幸福 Linux

红旗 Linux 是在 Linux 内核的基础上，经国内最大的 Linux 厂商—中科红旗软件技术有限公司开发出来的多用户、多任务的操作系统，它不仅包含有 Linux 内核，而且包含了大量的系统工具、开发工具、应用软件、办公组件及网络工具等，是一个面向企业和政府的 Internet/Intranet 综合应用平台。目前，红旗 Linux 的产品，已通过技术鉴定和公安部认证。联想集团正在和它进行大量合作，共同为政府提供“整体、安全的平台级解决方案”。

按照用户的使用目的不同，红旗 Linux 分为嵌入式系统、桌面系统和服务器系统。服务器系统目前的版本是 Red Flag Server 4.0。Red Flag Server 4.0 的功能主要体现在以下 4 个方面。

（1）支持多种不同的网络通信协议，包括 IPv4、IPv6、NetBIOS SMB 服务器消息块、IPX/SPX、广域网络（WAN）通信协议（X.25，Frame-relay 等）、ISDN/ADSL、PPP/SLIP/PLIP、业余无线电通信协议、ATM 通信协议、AppleTalk 通信协议、无线局域网协议 IEEE 802.11x、Web 协议

HTML/CSS/WSDL、由应用层软件 libxml 支持 XML 语言、服务质量协议 QoS，以及由 ITU-T 制订的目录服务的工业标准 X.500/LDAP。

(2) 支持多种不同的 Internet/Intranet 服务与应用，包括 Apache Web 服务器、Sendmail 电子邮件服务器、Proftpd 服务器、域名服务系统(DNS)服务、DHCP 动态主机配置协议、Samba 文件与打印共享、Squid 代理服务器、网络信息服务(NIS)、Nfs-utils 网络文件系统、Route 路由服务、集群应用、Mysql、Postgresql 数据库服务以及 Xinetd 超级服务器。

(3) 支持远程执行应用程序服务，包括 SSH 安全、shell 连接、Telnet 远程访问、X Window 远程执行方式、虚拟网络计算方式等。

(4) 支持网络互联，包括：路由器(Router)、网桥(Bridge)、IP 伪装(Masquerading)功能、记账(Accounting)功能、IP 别名(Aliasing)功能、网络流量控制(Traffic Shaping)功能、防火墙(Firewall)功能、端口转发(Port Forwarding)功能、负载平衡(Load Balancing)功能、串行连线的负载均衡驱动程序(EQL)、代理服务器(Proxy Server)、拨号(Dialed on Demand)服务功能、虚拟专用网(VPN)、网络管理工具。

4.3.2 Red Flag Server 4.0 的安装

1. 启动安装程序

(1) 将红旗 Red Flag Server 4.0 安装光盘放入 CD-ROM，重新启动计算机。

(2) 成功引导后将出现 Red Flag Server 4.0 的安装启动界面，屏幕显示提示信息和 boot：提示符。

如果需要使用专家安装方式，那么在“boot：”提示符下输入 expert，然后按 Enter 键。

通常情况下，直接按 Enter 键，使用默认的选择即可，以便安装程序可对计算机的硬件进行自动检测。如果安装程序没有正确地检测到硬件，需要使用专家(expert)模式重新启动安装程序，以提供额外的驱动程序。

(3) 按 Enter 键，选择默认的安装方式。安装程序将对计算机的硬件进行自动检测，然后进行 Linux 核心的启动。屏幕中出现 running/sbin/loader，如图 4-71 所示，表示正在运行安装程序的加载程序，也表示当前已经完成安装核心的启动。等待片刻后，就会进入图形安装界面。

2. 安装类型选择

(1) 完成安装程序的引导，进入图形化安装界面。Red Flag Server 4.0 提供统一的图形化安装界面，屏幕左侧列出了整个安装过程要经历的每一个步骤，并显示出当前所处的安装步骤；屏幕右侧是对应安装步骤的配置选项和参数设置界面。首先看到的是“红旗 Linux 软件协议书”，选择“同意”单选按钮，然后单击“下一步”按钮，如图 4-72 所示。

```
md driver 0.90.0 MAX_MD_DEVS=256, MAX_REAL=12
raid5: measuring checksumming speed
raid5: MMX detected, trying high-speed MMX checksum rout
   pII_mmx    :    220.599 MB/sec
   p5_mmx     :    225.171 MB/sec
   8regs      :    377.571 MB/sec
   32regs     :    200.787 MB/sec
using fastest function: 8regs (377.571 MB/sec)
scsi : 0 hosts.
scsi : detected total.
md.c: sizeof(mdp_super_t) = 4096
Partition check:
 hda: hda1 hda2 < hda5 >
RAMDISK: Compressed image found at block 0
VFS: Mounted root (ext2 filesystem).
Greetings.
Red Flag install init version 2.0 starting
mounting /proc filesystem... done
mounting /dev/pts (unix89 pty) filesystem... done
checking for NFS root filesystem...no
trying to remount root filesystem read write... done
checking for writeable /tmp... yes
running install...
running /sbin/loader
```

图 4-71　正在运行安装程序的加载程序



图 4-72　软件许可协议

（2）系统将显示安装类型选择界面，此时需要确定自己的工作任务，是选择“安装红旗操作系统”还是“恢复系统引导”。默认的选项是“安装红旗操作系统”。然后再进一步选择适合的安装类型：“典型安装”和“完全安装”。典型安装包含了主要的常用应用软件和软件包组，是默认的安装类型。完全安装增加了一些系统工具、实用程序以及开发工具和开发环境。通常，选择“典型安装”即可，如图 4-73 所示。



图 4-73　选择安装类型

3. 配置分区

完成安装类型的选择后，开始进行安装过程中最重要的步骤：配置分区。在此步骤中，必须告诉安装程序要在哪里安装系统，即为将要安装 Red Flag Server 4.0 的一个或多个磁盘分区上定义挂载点。这时，需要根据实际情况创建、修改或删除分区。

1）分区的命名

Linux 通过字母和数字的组合来标识硬盘分区。具体如表 4-5 所示。

例如：/dev/hda3 是指第一个 IDE 硬盘上的第三个主分区或扩展分区；/dev/sdb6 是第二个 SCSI 硬盘上的第二个逻辑分区。

注意：如果硬盘上没有分区，则一律不加数字，代表整块硬盘。

表 4-5　分区的命名

字母或数字	含义	说明
前两个字母	分区所在设备类型	hd:IDE 硬盘 sd:SCSI 硬盘
第三个字母	分区在哪个设备上	hda:第一块 IDE 硬盘 hdb:第二块 IDE 硬盘 sdc:第三块 SCSI 硬盘
数字	分区次序	数字 1～4 表示主分区或扩展分区，逻辑分区从 5 开始

2）分区的组织

分区的目的是在硬盘上为系统分配一个或几个确定的位置，Linux 系统支持多分区结构，分区的功能如表 4-6 所示，每一部分可以存放在不同的磁盘或分区上。

表 4-6　分区功能

分区	功能
/	整个系统的基础（必备）
swap	操作系统的交换空间（必备）
/boot	在根下创建，用来单独保存系统引导文件
/usr	用来保存系统软件
/home	包含所有用户的主目录，可保存几乎所有的用户文件
/var	保存邮件文件、新闻文件、打印队列和系统日志文件
/tmp	用来存放临时文件。对于大型、多用户的系统和网络服务器有必要

一般情况下，服务器系统都会规划多个分区，这样可以获得较大的灵活性和系统管理的方便性。安装 Red Flag Server 4.0 至少需要创建以下两个分区：

(1) 根分区（/）：Linux 根文件系统驻留的地方。

(2) 交换分区（swap）：用来支持虚拟内存的交换空间，当没有足够的内存来处理系统数据时，就要使用交换分区的空间。交换分区的大小建议设置为计算机内存的 1～2 倍之间。

至于如何规划服务器上的 Linux 硬盘空间，通常应考虑如下几个因素：

首先，Linux 根文件系统需要一部分的硬盘空间，挂载为“/”的根分区。其次，交换分区需要一部分的硬盘空间。交换分区的大小取决于需要多少虚拟 RAM。一般来说，交换分区的大小为物理 RAM 的 1～2 倍。最后，作为服务器用途，建议根据实际情况将根分区与 /usr、/home、/var、/boot 等分区单独放在不同的磁盘分区或设备上，这是因为将每个关键性的区域存放在独

立的分区，可为日后的移植、备份、系统恢复与管理提供方便。

3）选择分区方式

（1）图 4-74 是进入配置分区的界面，可以选择“用 Disk Druid 手工分区”或“用 fdisk 程序手工分区（只限专家）”进行分区操作。“用 Disk Druid 手工分区”提供图形化的操作界面，操作起来很直观，可以自由增加、编辑或删除分区；“用 fdisk 程序手工分区（只限专家）”是字符方式的设置工具，它的使用有一定难度，与 Windows 或 DOS 下的 fdisk 软件有很大的区别，通常有经验的用户才选择它。本书只讲述使用“用 Disk Druid 手工分区”进行分区的方法。



图 4-74　分区方法选择

（2）图 4-75 就是进入 Disk Druid 工具的界面，在此可以根据用户的要求创建、修改和删除硬盘分区，并对每个分区设置装入点。

可以看到，系统当前的硬盘分区情况以树状的目录层次结构列出，最上面的一级是硬盘，如果存在多个硬盘，分别以 hda、hdb、sda、sdb、… 表示；接下来的是硬盘上的主分区和扩展分区；最后是扩展分区下面的逻辑分区。

如果分区设备名前面带有“＋”号，表示它下面还包含有未显示的分区；如果分区设备名前的符号为“－”号，表示它下面的分区已全部显示。

分区列表中显示了系统中硬盘驱动器的详细信息，每一行代表一个硬盘分区，包括 5 个不同的字段，如表 4-7 所示。

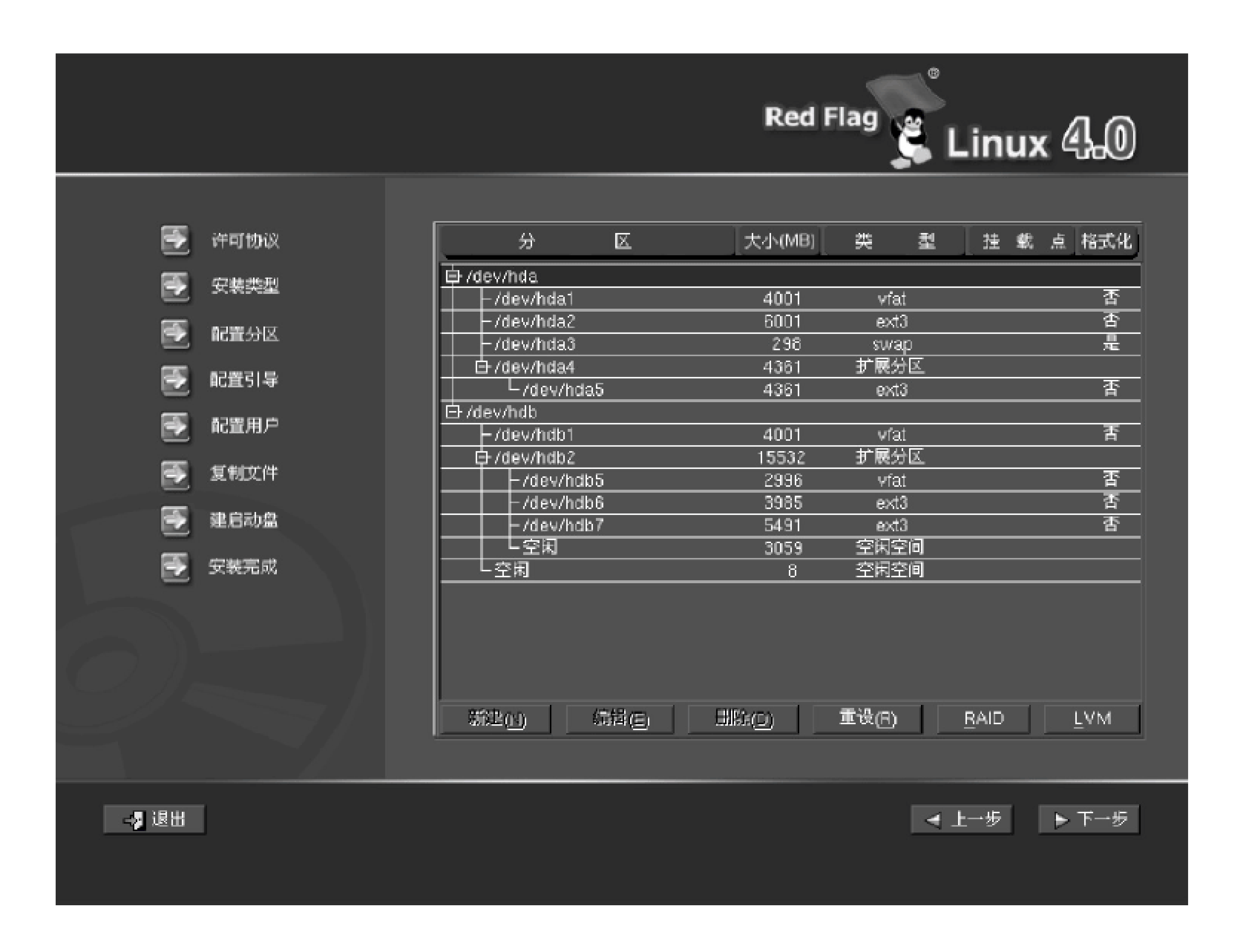


图 4-75　Disk Druid 分区工具

表 4-7　分区字段

字段	说明
分区	显示当前硬盘分区的名称
大小	当前分配给这个分区的空间(以 MB 为单位)
类型	显示了分区的文件系统类型
挂载点	指明分区在目录树中的加载位置
格式化	显示是否要对当前的分区进行格式化

分区列表底部的一排按钮用来控制 Disk Druid 的行为，每个按钮的用途如表 4-8 所示：

表 4-8　Disk Druid 分区工具功能按钮

按钮	用途
新建	在空闲分区上申请一个新分区。单击该按钮出现一个对话框，按要求输入所需的项
编辑	选中分区后，单击该按钮用来修改当前分区表中已创建好的分区的某些属性
删除	用来删除所选的分区
重设	取消所做的修改，将分区信息恢复到用户设置之前的布局
RAID	用来给部分或全部磁盘分区提供冗余性
LVM	只有具备 RAID(磁盘冗余阵列)的相关经验的用户才使用

（3）删除分区。如果硬盘上没有剩余的磁盘空间，或者是可以重新设置的 Linux 类型分区，那么需要先删除原有的分区，为安装 Red Flag Server 4.0 提供足够的空间。例如，要删除主机中已经存在的一个 Windows 分区，可以先在当前分区列表中选中该分区，然后单击“删除”按钮。

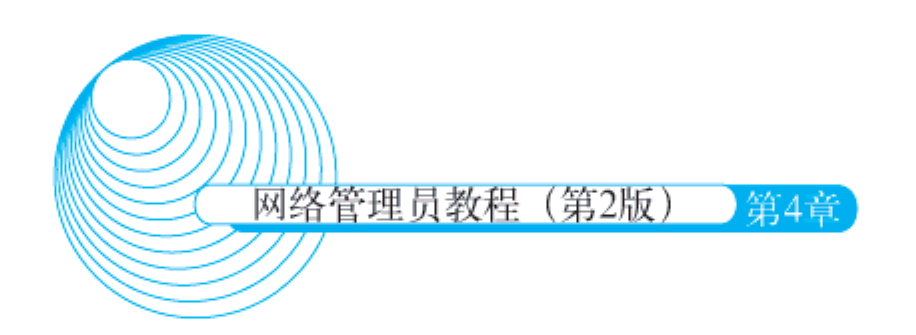
（4）添加新分区。在分区列表中选定空闲空间，双击或单击“新建”按钮，出现如图 4-76 所示对话框。其中每一个选项的功能如表 4-9 所示。当所有选项操作正确完成后，单击“下一步”按钮。



图 4-76　创建新分区

表 4-9　创建分区功能选项

选项名	功能
挂载点	输入将创建的分区在整个目录树中的位置，可以从下拉菜单中选择正确的挂载点。如果创建的是根分区，输入“/”；如果是交换分区，不需要输入装入点；如果创建的是根文件系统和交换分区以外的分区，应根据实际情况输入，如/boot、/home 等
文件系统类型	在提示列表中选择将创建分区的文件系统类型，如果创建的是交换分区，选择 swap；如果创建的是根文件系统或其他分区，可选择 ext3、reiserfs、jfs 或 ext2，默认的类型为 ext3
允许的驱动器	包括了系统上安装的硬盘列表。硬盘被突出显示表示在该硬盘上可以创建想要的分区。如果某个硬盘没有突出显示，那么这个分区一定不会在该硬盘上被创建
大小(MB)	输入分区的大小(以 MB 为单位)
使用全部可用空间	如选中该项，上面添入的分区大小将是该分区的最小值，指定的 Linux 分区将占据整个剩余硬盘空间。如果后面再创建分区时也使用这个选项，系统将根据这两个分区最小值的比例自动分配空间大小
检查磁盘坏块	如选中该项，会在格式化的过程中检查坏磁道，并将其列表以防今后被使用，这会花费更多的安装时间



Red Flag Server 4.0 允许根据分区将使用的文件系统来创建不同的分区类型。表4-10 是对不同文件系统以及它们的使用方法的简单描述。

表 4-10　文件系统

文件系统	使用方法
ext2	支持标准 UNIX 文件类型(常规文件、目录、符号链接等)。支持长达 255 个字符的文件名
ext3	ext2 的升级版本,可方便地从 ext2 迁移至 ext3。主要优点是在 ext2 的基础上加入了记录数据的日志功能,且支持异步的日志
reiserfs	一种新型的文件系统,通过完全平衡树结构来容纳数据,包括文件数据,文件名以及日志支持。Reiserfs 支持海量磁盘和磁盘阵列,并能在上面继续保持很快的搜索速度和很高的效率
jfs	IBM 的 jfs 文件系统提供了基于日志的字节级文件系统,该文件系统是为面向事务的高性能系统而开发的,与非日志文件系统相比,它的优点是其快速重启能力
物理卷(LVM)	创建一个或多个 LVM 分区,用于创建一个或多个 LVM 的逻辑卷
软件 RAID	创建两个或多个软件 RAID 分区,用于创建一个或多个 RAID 设备
swap	用于支持虚拟内存的交换空间
vfat	与 Windows 9x/2000/NT 的 FAT 文件系统的长文件名兼容的文件系统

(5) 编辑分区。选择当前分区列表中的一个分区,单击“编辑”按钮,将出现一个与图 4-76 类似的对话框,在对话框中修改此分区的设置。

如果一个分区已经存在于硬盘上时,那么只能修改这个分区的挂载点和文件系统类型。要想进行其他修改,如改变大小,就必须先删除这个分区然后重建。

4. 软 RAID 配置

1) RAID 的概念

RAID(Redundant Arrays of Inexpensive Disks)称为独立磁盘冗余阵列。RAID 的基本想法就是把多个便宜的小磁盘组合到一起,成为一个磁盘组,使性能达到或超过一个容量巨大、价格昂贵的磁盘。这样的磁盘组对于计算机来说,就像一个单独的逻辑存储单元或磁盘。

采用 RAID 的主要优势在于:

- 加快了磁盘速度;
- 扩充了存储能力;
- 可高效恢复磁盘。

2) RAID 的级别

(1) RAID 级别 0:通常称为“带区”。它利用了带区数据映射技巧的特定性能,也就是说,当

数据写入磁盘组的时候，被分成带区，交错写入磁盘组的磁盘中。这带来了高I/O性能，低开销，但不提供任何冗余。磁盘组的存储量等于总的磁盘容量之和。

(2) RAID级别1：即“镜像”，与RAID其他的各级别相比，这个级别使用的时间较长。1级通过把同样的数据写到磁盘组的每一个磁盘上，将镜像复制到每个磁盘上，来提供数据冗余。1级在读数据操作时，并行处理2个或更多的磁盘，因此数据传输速率高，但其他操作时无法提供高速的I/O传输速率。1级提供了非常好的数据的高可信度，并且改善了读数据操作的性能，但是，耗费很大。如果组成磁盘组的各磁盘规格相同，磁盘组的容量只等于一块磁盘的容量。

(3) RAID级别4：采用奇偶校验，但不提供冗余。它的数据分布在各个磁盘上，有一块盘作为奇偶校验盘。它更适用于I/O传输，而不是大文件传输。因为提供奇偶校验的磁盘常成为瓶颈，所以在没有相应技术的情况下，如回写高速缓存技术，不常使用4级。如果组成磁盘组的各磁盘规格相同，磁盘组容量等于构成磁盘组的磁盘的总容量，减去一块磁盘的容量。

(4) RAID级别5：这是一种最常用到的RAID类型。通过把奇偶校验分布到磁盘组中的一些或所有磁盘上，消除了4级在写数据上的瓶颈。在4级中，读的性能超过了写，性能是不对称的。5级常使用缓冲技术来降低性能的不对称性。如果组成磁盘组的各磁盘规格相同，磁盘组容量等于磁盘的总容量，减去一块磁盘的容量。由于RAID5与RAID4的容量相同，而性能优异，所以一般都使用RAID5。

(5) 线性RAID：线性RAID是为创建一个大型虚拟驱动设备而建立的简单的磁盘分组。在线性RAID中，磁盘上的带区是连续分配的，当第一块磁盘分配满后，跳转到下一块磁盘上，依次类推。这个磁盘组未做性能方面的改善，各种I/O操作都被划分到各磁盘上是不可靠的。线性RAID无冗余，并且可靠性降低。如果磁盘组中的任何一块磁盘出现故障，全部的阵列就都无法使用了。其容量是所有组成磁盘组的磁盘的容量之和。

3) RAID的实现方法

通常有两种可以实现RAID的方法：硬件RAID和软件RAID。

硬件RAID建立在硬件基础之上，与系统和主机无关，管理着RAID子系统。对于主机来说，每一个RAID组只是一个单独的硬盘。例如，硬件RAID设备通常是关联到一个SCSI控制器，RAID组看起来就是一个SCSI驱动器。外置的RAID磁盘柜把所有的RAID智能化地统一到外置磁盘子系统的控制器中。全部的子系统通过一个普通的SCSI控制器连到主机上，对主机来说，它就如同是一个单独的硬盘。

软件RAID通过核心磁盘(块设备)代码来实现不同的RAID级别，提供了最廉价的解决方案。不仅不再需要昂贵的磁盘控制器卡和热交换底盘，而且软件RAID在便宜的IDE硬盘上工作和在SCSI硬盘上一样好。加上现今的高速CPU，软件RAID的性能已超越了硬件RAID。

4) 创建RAID

安装 Red Flag Server 4.0 时，在“配置分区”步骤中可以方便地为系统划分 RAID 分区，创建 RAID 设备并将其格式化。已创建好并激活的 RAID 设备可以挂载到系统中，就像一个普通硬盘分区一样使用。对于已创建的 RAID 设备，也可以从系统中卸载、停用和删除。如果在安装时没有创建 RAID 设备，也可以在系统的使用过程中再添加或修改磁盘分区，创建需要的软件 RAID 设备。

(1) 在建立一个 RAID 设备之前，必须首先创建软件 RAID 分区。

在 Disk Druid 分区工具界面中，单击“新建”按钮以创建一个新的分区，出现“添加新分区”对话框，如图 4-77 所示。

① 此处不能输入挂载点，只有已经创建了软件 RAID 设备后才能为其设置挂载点。

② 在“文件系统类型”的选择列表中单击 software RAID。

③ 在“允许的驱动器”选项中选择将在其上建立 RAID 的硬盘。如果机器上带有多个硬盘，此处默认会全部选中，如果一定不会在某一硬盘上建立 RAID 阵列，必须取消对该硬盘的选中。

④ 在“大小(MB)”文件框中输入分区的大小(以 MB 为单位)。

⑤ “使用全部可用空间”：如选中该复选框，上面添入的分区大小将是该分区的最小值，指定的 Linux 分区将占据整个剩余硬盘空间。如果后面再创建分区时也使用这个选项，系统将根据这两个分区最小值的比例自动分配空间大小。

⑥ “检查磁盘坏块”：如选中该复选框，安装程序将在格式化分区之前检查坏磁道。

(2) 全部选项输入正确后，单击“确定”按钮返回到 Disk Druid 分区工具的主界面。重复上述步骤，创建其他需要制作为软件 RAID 设备的分区。

(3) 已经将所有需要制作成 RAID 设备的分区创建为 software RAID 分区后，开始建立 RAID 设备。在 Disk Druid 工具的主界面中，单击 RAID 按钮，出现图 4-78 所示的“建立 RAID 设备”对话框。

(4) 输入或从下拉菜单中选择该设备的挂载点。

(5) 在“文件系统类型”中选择 RAID 设备将采用的文件系统类型，默认的类型是 ext3。

(6) 在“RAID 级别”中，可以选择建立 RAID0、RAID1 或 RAID5；如果要将 RAID 设备挂载到/boot 上，则必须选择 RAID1 级别；同理，如果不打算创建单独的/boot 分区，而是将整个/分区建立成 RAID 设备，那么也必须选择 RAID1 级别。

(7) 在“RAID 成员”列表中，显示用于创建的 RAID 设备的分区，可以选择要使用哪几个分区来建立 RAID 设备。

(8) 单击“确定”按钮，新建的软件 RAID 设备将显示在 Disk Druid 工具主界面的分区列表中，如图 4-79 所示。

5. LVM 配置

1) LVM 的概念



图 4-77 创建一个新的 RAID 分区



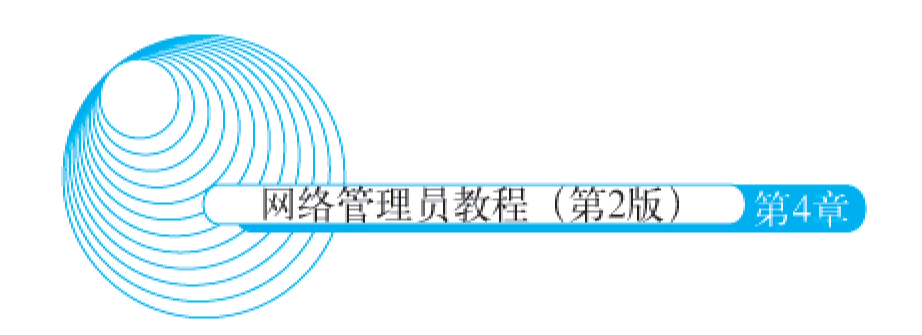
图 4-78 建立 RAID 设备

分区	大小(MB)	类型	挂载点	格式化
RAID Device 0	1498	ext3	/home	是
/dev/hda				
/dev/hda1	4001	vfat		否
/dev/hda2	6001	ext3		否
/dev/hda3	298	swap		是
/dev/hda4	4361	扩展分区		
/dev/hda5	4361	ext3		否
/dev/hdb				
/dev/hdb1	4001	vfat		否
/dev/hdb2	15532	扩展分区		
/dev/hdb5	2996	vfat		否
/dev/hdb6	3985	ext3		否
/dev/hdb7	5491	ext3		否
/dev/hdb8	1498	软件 RAID		
/dev/hdb9	1498	软件 RAID		
空闲	63	空闲空间		
空闲	8	空闲空间		

新建(N) 编辑(E) 删除(D) 重设(R) RAID LVM

图 4-79 RAID 磁盘阵列已建立

LVM 是 Logical Volume Manager 的简写，它为计算机提供了更高层次的磁盘存储解决方



案，使系统管理员可以更方便地分配存储空间。Red Flag 可以根据需要将一个或多个硬盘分区创建为用于 LVM 的物理卷，已创建的软件 RAID 设备也可以设置为物理卷。

(1) 卷组(VG，Volume Group)：LVM 中最高抽象层，由一个或多个物理卷所组成的存储器池。

(2) 物理卷(PV，Physical Volume)：典型的物理卷是硬盘分区，也可以是整个硬盘或已创建的软件 RAID 设备。

(3) 逻辑卷(LV，Logical Volume)：相当于非 LVM 系统中的分区，它在卷组上建立，是一个标准的块设备，可以在其上建立文件系统。

(4) 物理块(PE，Physical Extent)：物理卷以大小相等的“块”为单位存储，块的大小与卷组中逻辑卷块的大小相同。

(5) 逻辑块(LE，Logical Extent)：逻辑卷以“块”为单位存储，在一卷组中的所有逻辑卷的块大小是相同的。

2) LVM 的优点

传统的文件系统是基于分区的，一个文件系统对应一个分区。这种方式比较直观，但不易改变：不同的分区相对独立，各分区空间经常利用不平衡，空间不能充分利用；当一个文件系统/分区已满时，无法对其扩充，只能重新分区，或把分区中的数据移到另一个更大的分区中，非常麻烦；要把硬盘上的多个分区合并在一起使用，只能采用重新分区的方式，这个过程需要数据的备份与恢复。当采用 LVM 时，情况会有所不同：

(1) 硬盘的多个分区由 LVM 统一为卷组管理，可以方便的加入或移走分区以扩大或减小卷组的可用容量，硬盘空间被充分利用。

(2) 文件系统建立在逻辑卷上，而逻辑卷可在卷组容量范围内根据需要改变大小。

(3) 文件系统建立在 LVM 上，可以跨分区，使用方便。

(4) 在一个有很多不同容量硬盘的大型系统中，用户/用户组的空间建立在 LVM 上，可以随时按要求增大，或根据使用情况对各逻辑卷进行调整。

(5) 当系统空间不足而加入新的硬盘时，不必把用户的数据从原硬盘迁移到新硬盘，而只须把新的分区加入卷组并扩充逻辑卷即可。

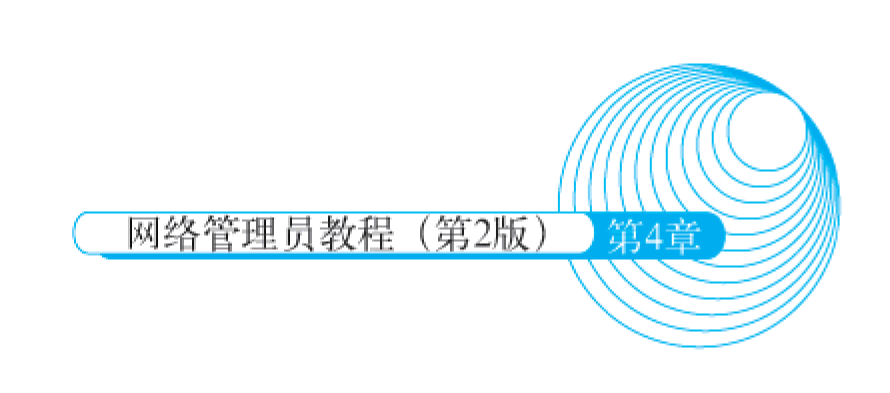
(6) 使用 LVM 可以在不停止服务的情况下，把用户数据从旧硬盘转移到新硬盘空间。

3) LVM 的使用

创建和配置 LVM 逻辑卷的步骤包括以下几步：

(1) 在创建一个 LVM 逻辑卷之前，必须首先选择和创建用于 LVM 的物理卷，只有这样它们才可以被 LVM 系统识别。

(2) 由一个或多个物理卷创建卷组，卷组可以看作是由一个或多个物理卷所组成的存储



器池。

（3）在卷组上创建逻辑卷，在逻辑卷上安装和创建文件系统，为逻辑卷设置挂载点。

需要指出的是：可以在一个卷组上创建多个逻辑卷，但是一个物理卷只能属于一个卷组。/boot 分区不能建立在卷组上，如果要将根文件建立上一个逻辑卷上，那么必须在非逻辑卷分区上单独为/boot 划分一个分区。

4）创建 LVM

（1）在硬盘分区上选择并初始化用于 LVM 的物理卷。在 Disk Druid 分区工具界面中，单击“新建”按钮以创建一个新的分区；出现“添加新分区”对话框，如图 4-80 所示。在“文件系统类型”的选择列表中单击 physical volume（LVM）。此处不能输入挂载点，只有创建了 LVM 卷组后才能为其上的逻辑卷设置挂载点。

（2）建立 LVM 卷组。在图 4-75 所示的 Disk Druid 工具的主界面中，单击 LVM 按钮，将一个或多个物理卷组成一个卷组，如图 4-81 所示。可以在“卷组名称”文本框中改变卷组的名称；LVM 逻辑卷以大小相等的“块”为单位分配存储量，4MB 是默认的大

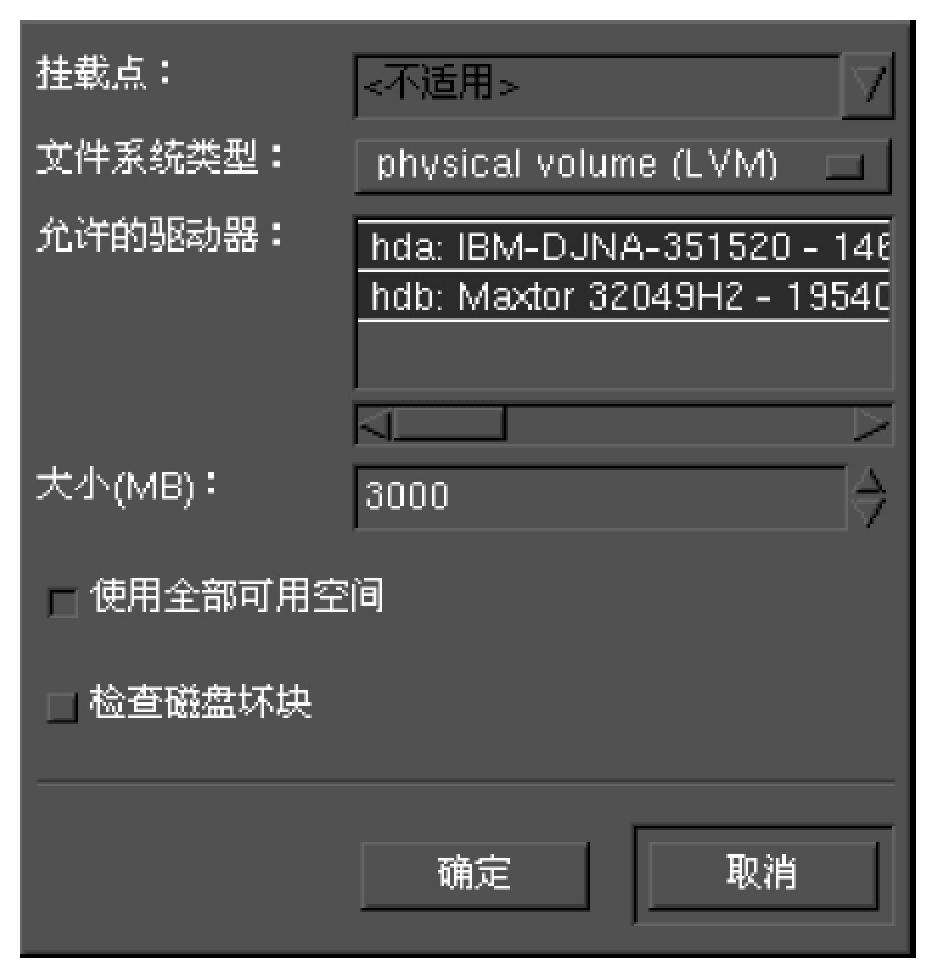


图 4-80　创建一个物理卷



图 4-81　创建一个 LVM 卷组

小，这样逻辑卷的空间一定是4MB的整数倍。可以从“物理范围”选择列表中选择其他值，建议不要改变默认设置；在“要使用的物理卷”列表中选择组成本卷组的物理卷。

（3）在卷组上创建逻辑卷。在“逻辑卷”区域，单击“添加”按钮，出现如图4-82所示的界面，用于在已建立的卷组上创建新的逻辑卷，并为其设置挂载点、指定文件系统类型、确定名称和分配空间。当然，也可以对逻辑卷进行编辑和删除操作。在创建逻辑组时应考虑在卷组上留有一些空闲空间，以方便今后对逻辑卷进行扩展。



图 4-82　创建一个逻辑卷

（4）单击“确定”按钮，新建的LVM卷组和逻辑卷将显示在Disk Druid工具主界面的分区列表中，如图4-83所示。

分区	大小(MB)	类型	挂载点	格式化
LVM VG				
Volume00	3059	LVM VG		
LogVol00	1500	ext3	/home	是
/dev/hda				
/dev/hda1	4001	vfat		否
/dev/hda2	6001	ext3		否
/dev/hda3	298	swap		是
/dev/hda4	4361	扩展分区		
/dev/hda5	4361	ext3		否
/dev/hdb				
/dev/hdb1	4001	vfat		否
/dev/hdb2	15532	扩展分区		
/dev/hdb5	2996	vfat		否
/dev/hdb6	3985	ext3		否
/dev/hdb7	5491	ext3		否
/dev/hdb8	3059	LVM PV		是
空闲	8	空闲空间		

新建(N)　编辑(E)　删除(D)　重设(R)　RAID　LVM

图 4-83　Logical Volumes 已建立

6. 配置引导

引导装载程序在计算机启动时首先运行，负责载入操作系统内核并把控制权转交给它。LILO(LInux LOader)是Red Flag Server 4.0的启动引导程序，它支持Red Flag Server 4.0与多种操作系统共存，允许用户在系统启动时通过LILO菜单选择想要进入的操作系统。可以把LILO安装在以下两个位置之一：MBR(主引导记录)或者引导分区的第一个扇区(如/dev/

hda1）。

MBR 是硬盘上的一个特别的区域，会自动被 BIOS 装载，是引导装载程序控制引导进程最早的位置。建议尽可能地把 LILO 程序安装在主引导扇区内。

如果系统已经在使用其他启动管理器（如 System Commander、Boot Manager 等），才把 LILO 装在引导分区的第一个扇区中。这时需要设置从其他的启动管理器来启动 LILO，然后再启动 Red Flag Server 4.0。

如果系统只使用 Red Flag Server 4.0 系统，则应该选择 MBR；对于带有 Windows 9x/2000/NT 的系统来说，也应该把引导装载程序安装到 MBR。

LILO 配置界面如图 4-84 所示，LILO 配置工具的使用说明如下。

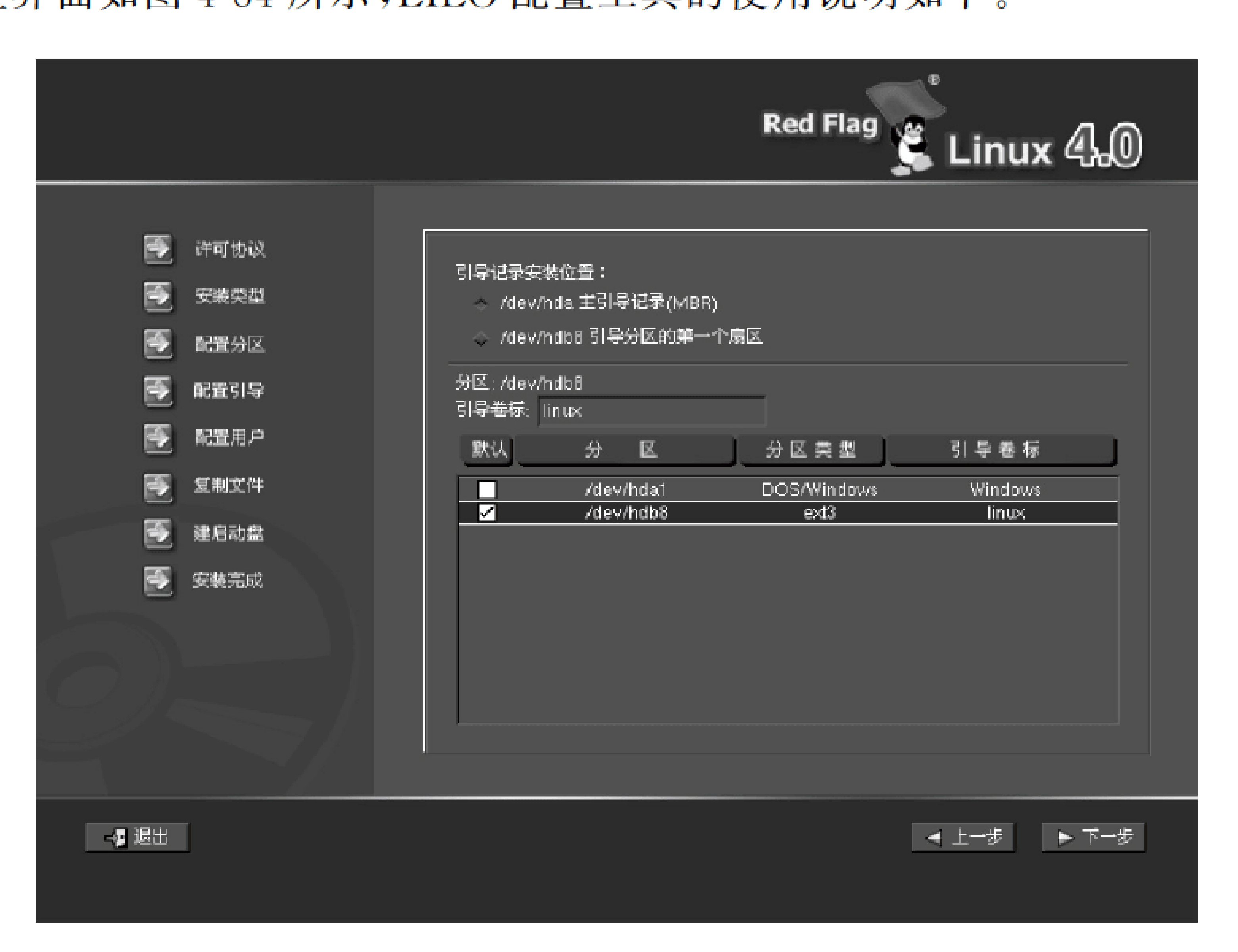


图 4-84　LILO 程序设置

（1）引导记录安装位置：用来设置安装 LILO 的位置。如上所述，可以选择在主引导记录中安装，也可以选择在引导分区的第一个扇区中安装。

（2）引导卷标：就是当 LILO 启动后，在菜单中显示的可引导操作系统的标识，或者是在非图形化引导装载程序的引导提示下输入的信息。

默认情况下，Red Flag Server 4.0 的引导卷标为 Linux，Windows 分区的启动卷标为 Windows。这些默认的引导卷标都是可以修改的。如果想为其他分区增加或修改引导卷标，只要用鼠标单击该分区，然后在“引导卷标”输入框中输入新的标识名称即可。

7. 配置用户

在如图4-85所示的安装步骤中，安装程序会提示设置系统的 root 密码，必须输入一个根口令，否则安装将无法继续。



图4-85　设定用户账号

对于 Linux 服务器系统来说，系统的 root 口令是决定系统安全性的重要参数。root 是系统管理者，可以对系统进行任意的操作，因此，root 口令的保密性要求很高。密码必须至少包括6个字符，并且是区分大小写的。系统管理员应记好自己的密码，并且养成定期更改密码的好习惯。

接下来可以建立一个或多个普通用户账号并为其设定口令。在此，系统管理员至少应给自己添加一个普通用户账号，供平常进入系统管理日常的工作。输入一个用户名，并为该用户设置口令，然后单击“添加”按钮，新用户的账号信息就会添加到用户列表之中。

8. 开始安装

完成用户的设置，开始正式安装之前，会进入如图4-86所示的安装确认界面。请确认前面的安装选项设置无误，这里是安装过程中最后一个可以单击“上一步”按钮返回或取消安装的地方；一旦单击“下一步”按钮，将正式开始格式化分区和安装软件包。



图 4-86　检查安装选项

9. 复制文件

首先，安装程序会读取需要安装的软件包信息，进行必要的准备工作，然后开始文件的复制过程。安装所需的时间由所选安装类型、硬件的速度、系统内存大小等多个方面确定，大概需要十几分钟到几十分钟不等。图 4-87 是安装过程中的一幅画面。屏幕左下方显示了安装的总体进度，屏幕右侧是对系统的简单介绍，可以在安装的过程中通过它们来了解 Red Flag Server 4.0 的系统特征。

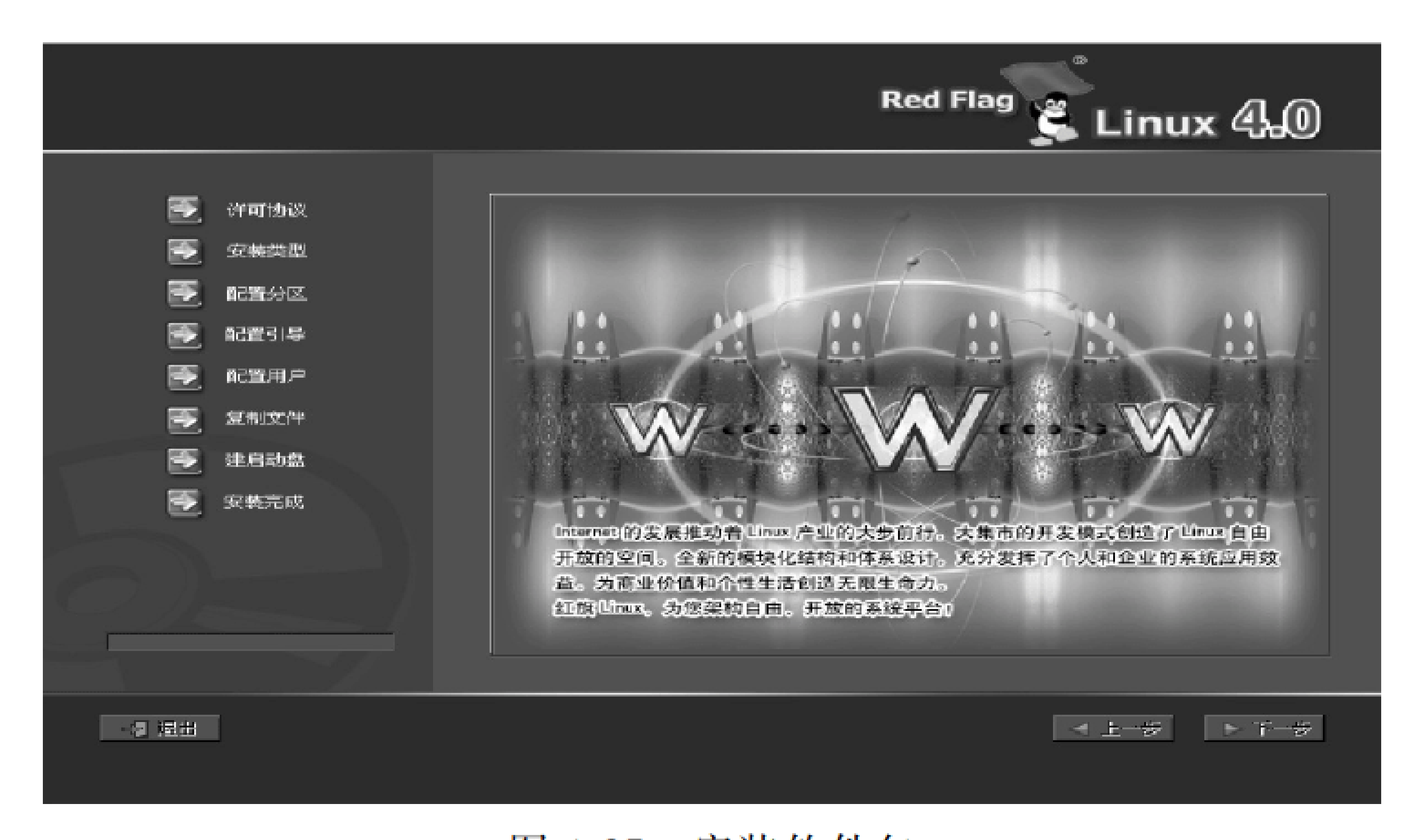
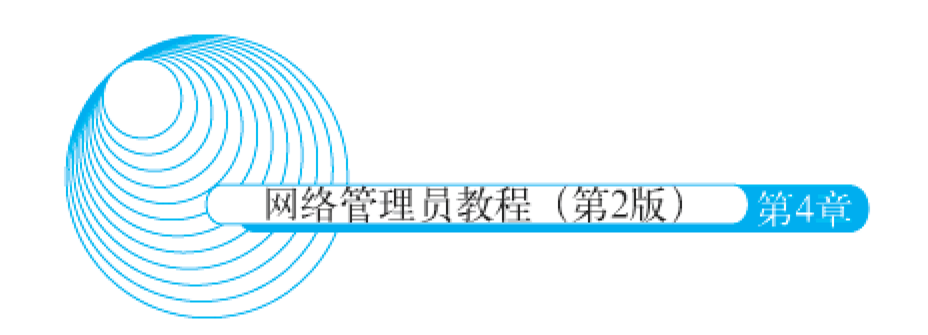


图 4-87　安装软件包



10. 创建引导盘

软件包复制完成后，会进入图4-88所示的制作系统引导软盘界面。引导盘会储存当前的系统设置，在系统出现问题时帮助用户引导和还原Red Flag Server 4.0系统，对于系统维护和故障排除具有重要的意义。建议用户在安装过程中建立引导软盘并妥善保存。在软盘驱动器中插入一张高质量的软盘，单击“下一步”按钮，继续引导软盘的制作。

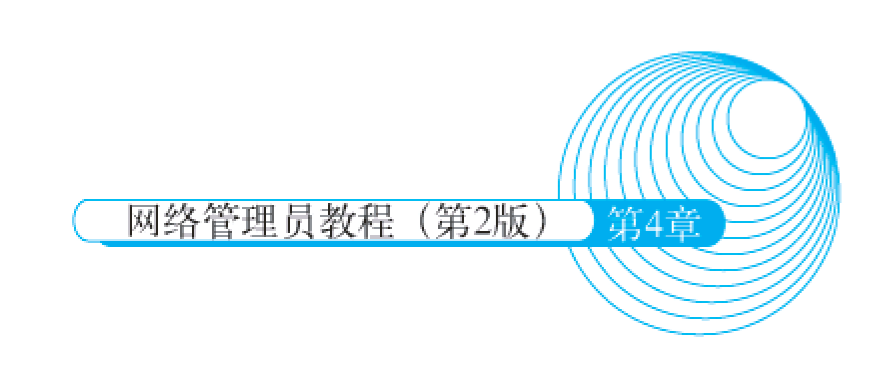


图4-88　制作引导软盘

引导软盘制作完成之后，Red Flag Server 4.0的安装即将结束。图4-89所示为安装完成的界面。至此已经成功地将Red Flag Server 4.0安装到计算机中了。按下计算机面板上光驱的“弹出”按钮，将弹出的光盘取出，重新启动系统。



图4-89　安装完成



4.3.3 Red Flag Server 4.0 的使用

安装完成后重新启动计算机，系统自检结束后会出现 LILO 启动引导菜单，如果计算机中已安装了红旗 Linux Desktop、红旗 Linux Server 和 Windows 98 3 个操作系统。打开计算机的电源，系统自检后，将显示出如图 4-90 所示的 LILO 启动菜单界面。使用键盘上的方向键可以选择想要启动的系统，按 Enter 键后，计算机将按照所选择的系统启动。

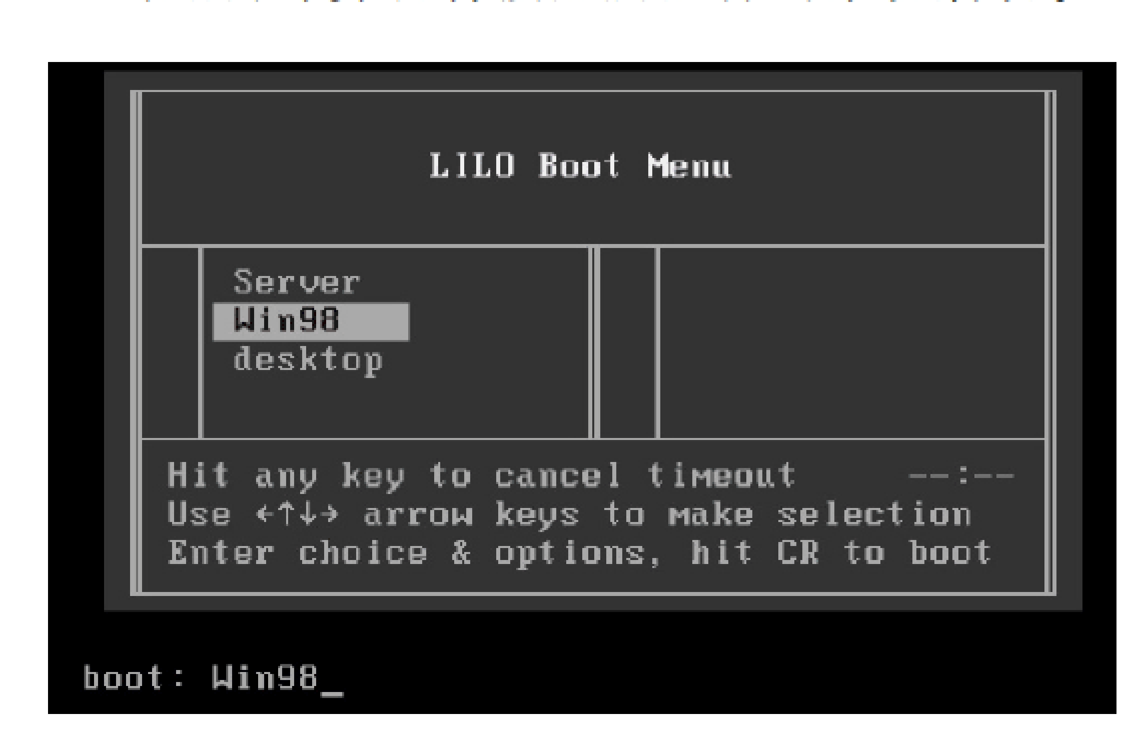


图 4-90 Linux 系统管理中的启动多操作系统

1. 开始和结束操作

1）登录

Linux 是一个多用户、多任务的操作系统，它允许多个用户共享系统的软硬件资源，不同用户对系统的使用权限和使用方式也不同，所以红旗 Linux 系统有一个对访问系统的用户进行识别和验证的过程，此过程称为登录（logging in，或注册）。简单地说，登录就是输入用户名和口令以表明自己是系统授权使用者的过程，这个步骤有助于维护系统的安全。

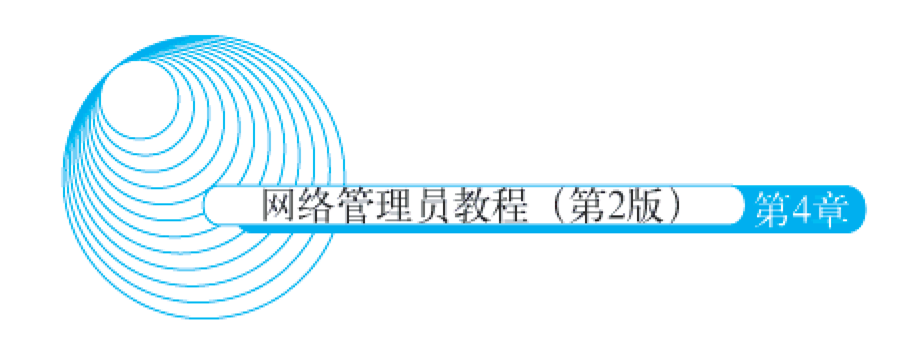
计算机加电自检结束，完成 LILO 的引导后，系统将会进行一系列的检测、设定，开启各项服务程序后进入 Red Flag Server 4.0 的登录界面。登录进入系统时，需要提供用户名在 login：提示符之后输入要登录系统的用户名，然后按 Enter 键。

用户名分为两种：一种是系统管理员使用的账号，也称为超级用户账号，用 root 表示，使用它可以在系统中做任何操作；另一种是普通用户账号，只能进行权限范围内的操作。

为了避免错误操作造成的损失，建议使用普通用户登录系统。如果在安装过程中没有创建其他用户账号，则必须在第一次登入系统时使用 root 身份登录，登录后再添加系统的普通用户账号。

当看到屏幕上出现“Password：”提示时，输入该用户的口令，然后按 Enter 键。

password 后输入的字符将不在屏幕上回显，光标也不移动，这是一种安全措施。防止别有



用心的人看到用户输入的口令。

只有授权的用户才能够登录进入系统，如果输入的用户名和口令都正确，系统会在屏幕上显示如下的 shell 提示符，表示登录成功。

[root@localhost /root] #（超级用户方式）

[Redflag@localhost Redflag] $（普通用户方式，此处用户名为 Redflag）

输入用户名、口令与命令名时，一定要区分大小写，因为大小写字母在 Linux 系统中代表不同的含义。

2）退出

当完成任务，想要退出系统时，在提示符后面输入命令 logout 或 exit，然后按 Enter 键，系统进行相应处理后，就会回到显示登录提示信息屏幕下。在 shell 提示符之后，同时按下 Ctrl＋D 键也可以退出系统。

3）关机和重新启动

在 Linux 系统中，不要在没有执行完正常关机程序的情况下关闭电源。否则在下次启动时，可能会看到系统报告磁盘有错误。系统管理员可以用 poweroff 命令关闭系统，用 reboot 命令重启系统。同时按下 Ctrl＋Alt＋Del 键，可以重新启动系统。

此外，shutdown 命令的使用更为灵活：输入没有参数的 shutdown 命令，2 分钟后即可关闭系统，shutdown 命令还可以加入一些参数选项：

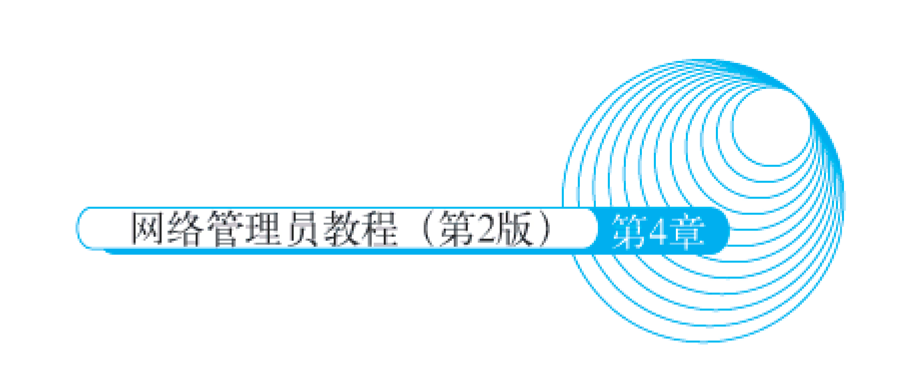
- now 表示立即。
- ＋mins 表示在指定分钟之后。
- hh：ss 表示在一个特定的时间内。
- poweroff 命令相当于 shutdown - h now。
- reboot 命令相当于 shutdown - r now。

2. 用户界面

用户界面是指用户与计算机交流的方式。Red Flag Server 4.0 提供了两种不同的用户界面：基于文本方式的命令行界面与图形化桌面环境两种。使用哪一种界面取决于用户的操作习惯及实际使用要求。

1）命令行界面

命令行界面是 Linux 系统中传统的用户界面，功能十分强大。用户进入 Red Flag Server 4.0环境时系统将自动启动相应 shell，shell 是一种命令行解释程序（command-language interpreter），负责用户和操作系统之间的沟通，在提示符下输入的每个命令都是由 shell 解释后传给 Linux 内核执行的。通过 shell 可以启动、挂起、停止甚至编写程序。Shell 的种类有很多，Red Flag Server 4.0 的默认 shell 是 bash。Bash 是 Bourne Again Shell 的缩写，在 bash 下，root



账号用“#”作为提示符，普通用户用“$”作为提示符。

2）KDE桌面环境

KDE是Red Flag Server 4.0中包含的一个功能强大的桌面系统。KDE是K Desktop Environment的缩写（K字母没有特定含义只是在顺序上排在D字母前边），是一套用于“UNIX工作站上的强大的图形工作环境”，它使Linux操作系统拥有图形化易用的桌面集成环境。Red Flag Server 4.0采用最新稳定的KDE 3.1.0作为标准的桌面环境，其细致友好、清新自然的图形操作环境会为用户带来前所未有的方便。

3）启动KDE

KDE桌面环境是Red Flag Server 4.0中默认的图形环境，用户在文本方式登录后，输入如下命令：

```
# startx
```

或

```
# startkde
```

系统将启动KDE桌面环境，这个过程可能会花几秒钟的时间。

4）注销KDE

通常使用以下方法注销桌面会话。单击桌面面板上的主菜单“开始”按钮，或使用快捷键Alt+F1打开系统主菜单，选择“注销”选项。也可以单击面板右侧的注销图标。

这时屏幕显示注销对话框，同时背景颜色变暗，要求用户确认是否注销本次登录。单击“注销”按钮结束桌面环境中的操作。如果还有未保存的作业，可以单击“取消”按钮，把当前需要保存的作业存盘，然后再退出。

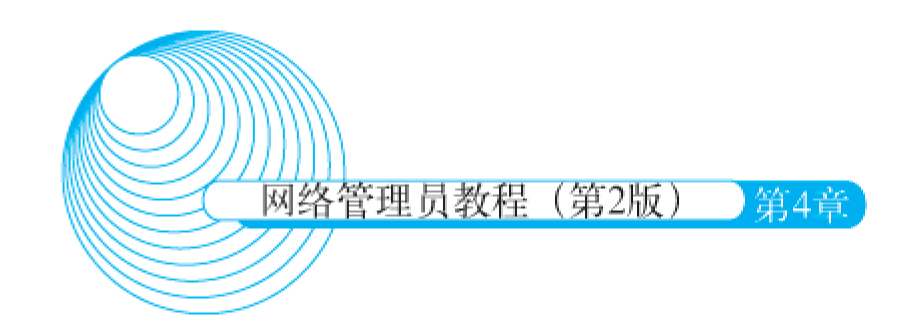
如果用以上介绍的方法无法退出，可以同时按下Ctrl+Alt+Back Space键，系统会立即关闭桌面窗口。

注意：一定要确保已经保存了所有的工作。

5）运行级别

运行级别（runlevel）是初始化进程在系统进入某运行级别时需要完成的启动或停止服务，它描述了系统能够提供什么服务和不能提供什么服务。运行级别是用数字来定义的，Red Flag Server 4.0中定义了7个运行级别，分别说明如下。

- 0：停止系统运行（不能将其设为默认运行级别）。
- 1：单用户模式，一般用于特别的系统管理工作，如root口令丢失、文件系统检查等。
- 2：多用户模式，但不支持网络文件系统（NFS）。
- 3：完全多用户模式。
- 4：系统保留，未定义。



• 5：多用户模式，相对 3 而言，默认以图形界面登录。
• 6：系统重新启动（不能将其设为默认运行级别）。

系统中关于初始化（init）进程最重要的配置文件是/etc/inittab，如果希望以图形方式登录，可以通过编辑/etc/inittab 文件，即将其中如下所示的一行：

```
id:3:initdefault:
```

改为：

```
id:5:initdefault:
```

它将系统的运行级别设为 5，即 X Window 启动方式，这时系统启动后将自动显示图形方式的登录界面，如图 4-91 所示。



图 4-91　图形登录界面

一种有趣的关机方法就是将系统切换到运行级别 0（停机）或运行级别 6（重新启动），例如，下面的命令将会关闭系统。

```
# init 0
```

3. 文件管理

1）文件命名

Linux 下文件名长度最大可以为 256 个字符，通常是由字母、数字、“.”（点号）、“_”（下划线）和“－”（减号）组成的。

注意：文件名不能含有“/”符号，因为“/”在 Linux 目录树中表示根目录或路径中的分隔符（如同 DOS 中的“\”）。

Linux 系统中支持文件名中的通配符，具体说明如下。

（1）星号（*）：匹配零个或多个字符。

（2）问号(?)：匹配任何一个字符。

（3）[ab1 A-F]：匹配任何一个列举在方括号中的字符。该集合是a、b、1或任何一个从A到F的大写字符。

2）路径

操作系统查找一个文件所经过的路径称为路径名。使用当前目录下的文件时可以直接引用文件名；如果要使用的是其他目录下的文件，就必须指定该文件所在的路径。

按查找文件的起点不同路径可以分为两种：绝对路径和相对路径。从根目录开始的路径称为绝对路径；从当前所在目录开始的路径称为相对路径。相对路径是随着用户工作目录的变化而改变的。

与DOS相同，每个目录下都有代表当前目录的"." 文件和代表当前目录父目录的".."文件，相对路径名就是从".." 开始的。不同的是，在Linux的目录树中表示根目录或是路径中的分隔符是"/" 。

3）文件类型

Red Flag Server 4.0系统支持以下文件类型：普通文件、目录文件、设备文件以及符号链接文件。

（1）普通文件：包括文本文件、数据文件、可执行的二进制程序等。

（2）目录文件：简称为目录，Linux中把目录看成是一种特殊的文件，利用它构成文件系统的分层树型结构。每个目录文件中至少包括两个文件，".."表示上一级目录，"."表示该目录本身。

（3）设备文件：设备文件是一种特别文件，Linux系统用来标识各个设备驱动器，核心使用它们与硬件设备通信。有两类特别设备文件：字符设备文件和块设备文件。

（4）符号链接：一种特殊文件，存放的数据是文件系统中通向某个文件的路径。当调用符号链接文件时，系统自动地访问保存在文件中的路径。

4）目录结构

通过对系统目录组织结构的了解，可以在进行文件操作和系统管理时方便地知道所要的东西在什么地方。Red Flag Server 4.0的文件系统采用分层的树型目录结构。即：在一个根目录(通常用"/" 表示)，含有多个下级子目录或文件；子目录中又可能含有更下级的子目录或者文件的信息；……这样一层一层地延伸下去，构成一棵倒置的树。树中的"根"与"杈"代表的是目录或称为文件夹，而"叶子"则是一个个的文件。

下面列出了主要的系统目录及其简单描述。

（1）/bin：存放普通用户可以使用的命令文件。目录/usr/bin也可用来贮存用户命令。

（2）/sbin：一般存放非普通用户使用的命令(有时普通用户也可能会用到)。目录/usr/sbin中也包括了许多系统命令。

（3）/etc：系统的配置文件。

（4）/root：系统管理员（root 或超级用户）的主目录。

（5）/usr：包括与系统用户直接相关的文件和目录，一些主要的应用程序也保存在该目录下。

（6）/home：用户主目录的位置，保存了用户文件（用户的配置文件、文档、数据等）。

（7）/dev：设备文件所在目录。在 Linux 中设备以文件形式表现，从而可以按照操作文件的方式简便地对设备进行操作。

（8）/mnt：文件系统挂载点。一般用于安装移动介质，其他文件系统（如 DOS）的分区、网络共享文件系统或任何可安装的文件系统。

（9）/lib：包含许多由/bin 和/sbin 中的程序使用的共享库文件。目录/usr/lib/中含有更多用于用户程序的库文件。

（10）/boot：包括内核和其他系统启动时使用的文件。

（11）/var：包含一些经常改变的文件。例如假脱机（spool）目录、文件日志目录、锁文件、临时文件等。

（12）/proc：操作系统的内存映像文件系统，是一个虚拟的文件系统（没有占用磁盘空间）。查看时，看到的是内存里的信息，这些文件有助于了解系统内部信息。

（13）/initrd：在计算机启动时挂载 initrd. img 映像文件的目录以及载入所需设备模块的目录。

（14）/opt：存放可选择安装的文件和程序。主要由第三方开发者用于安装他们的软件包。

（15）/tmp：用户和程序的临时目录，该目录中的文件被系统定时自动清空。

（16）/lost＋found：在系统修复过程中恢复的文件所在目录。

4. Shell 命令

1）Shell 简介

用户在命令行下工作时，不是直接同操作系统内核打交道，而是由命令解释器接受命令，分析后再传给相关的程序。进入 Red Flag Server 4.0 环境时系统将自动启动相应的 shell，shell 是一种命令行解释程序，它提供用户与操作系统之间的接口。Red Flag Server 4.0 下默认的 shell 是 bash。bash 命令的基本格式如下：

```
命令名[选项][参数 1][参数 2]…
```

其中方括号括起的部分表明该项对命令而言是可选的。

- [选项]：对命令有特别定义，一般以“-”开始，多个选项可用一个“-”连起来，如 ls -l -a 与 ls-la 相同。
- [参数]：提供命令运行的信息，或者是命令执行过程中所使用的文件名。

在使用 shell 命令时，要注意以下一些事项：

(1) 输入用户名、口令与文件名、命令名时，一定要区分大小写，因为大小写字母在 Linux 系统中代表不同的含义。

(2) 在命令、选项和参数之间要用空格隔开。连续的空格会被 shell 解释为单个空格。

(3) 在 shell 提示符下输入相应的命令，然后按 Enter 键确认，shell 会读取该命令并执行。如果系统找不到输入的命令，会显示 Command not Found，这时需要检查输入的命令的拼写及大小写是否正确。

(4) 使用分号(;)可以将两个命令隔开，这样可以实现在一行中输入多个命令。命令的执行顺序和输入的顺序相同。

(5) 当要输入的命令目录很深或命令中的文件名很长时，只要按一下 Tab 键，系统会在可能的命令或文件名中找到相匹配的项，自动补齐。如果有一个以上的文件符合输入的字符串，不能补齐时，可以按两下 Tab 键，系统将把所有符合的文件名列出来。

(6) shell 会把过去输入过的命令记忆下来，只要按上下方向键，就可以选择以前输入过的命令了。

有了以上基础，可以运行下面列出的几个简单命令来实际使用一下。

- clear：刷新屏幕。
- date：在屏幕上显示日期和时间。
- echo：将命令行中的内容回显到标准输出上。
- cal：显示月份和日历。

2) 系统帮助

Red Flag Server 4.0 具有强大的系统和网络功能，数量众多的实用工具软件和大量复杂的操作命令。为了帮助用户顺利进行操作，系统提供了多种多样的联机帮助信息以便用户随时查询。通过 man 命令使用联机用户手册，系统可以显示任何命令的联机帮助信息。它将命令名称作为参数，该命令的语法格式为：

```
man command
```

常用的 Linux 系统帮助手册的章节分类，它位于/usr/man 目录下。

例如，下面的命令行将显示 cal 命令的手册页。

```
$ man cal
```

使用命令 man man 会显示出 man 命令本身的使用方法。

在所查询的命令后加-help 参数的方式，也可以显示出命令的参考信息。

用 help command 可列出许多内部命令的帮助。

whatis 命令可以通过命令名查找简要的帮助信息，命令语法为：whatis keyword。

3）目录操作命令

（1）查看目录

查看目录内容的命令是ls，它默认显示当前目录的内容，可以在命令行参数的位置给出一个或多个目录名，从而可以查看这些目录。该命令的语法格式为：

```
ls [选项]…[文件名]…
```

ls命令有多个命令行选项，分别说明如下。

① -a：列出所有文件，包括那些以“.”开头的文件。

② -d：如果后面接的是一个目录，那么使用该参数只输出该目录的名称。

③ -l：使用长格式显示文件条目，包括连接数目、所有者、大小、最后修改时间、权限等。

④ -t：按文件修改时间进行排序，而不是使用文件名排序。

⑤ -C：按列纵向对文件名排序。

⑥ -F：在文件名后加上一个符号来表示文件类型。

⑦ -Cx：按行跨页对文件名排序。

⑧ -CF：按列列出目录中的文件名，该命令在文件名之后附加一个字符用来区分目录和文件的类型。

- 目录文件名之后附加一个斜线(/)。
- 可执行文件名之后附加一个星号(*)。
- 符号链接文件之后附加一个@字符。
- 普通文件名之后不加任何字符。

⑨ -CR：按多栏格式显示当前目录中的所有文件以及沿目录树向下各个子目录的所有文件，也称作递归列表。该命令可以区分目录和可执行的文件，即在文件名之后附加一个字符。

（2）改变工作目录

进入一个目录，或者说改变当前工作目录使用cd命令，其命令的语法格式为：

```
cd 目录名
```

cd命令带有唯一的一个参数，即表示目标目录的路径名(相对路径名或绝对路径名)。

利用两点“..”把工作目录向上移动一级目录：

```
cd ..
```

为了从系统中的任何地方返回到用户主目录，可以使用不带任何参数的cd命令。

（3）创建目录

使用mkdir命令创建一个目录或多个目录，以便有效地组织文件。其命令的语法格式为：

```
mkdir [选项] 目录名[目录名…]
```

同一子目录应包含类似的文件。例如，应建立一个子目录，包含所有的数据库文件；另一个子目录包含电子表格文件；还有一个子目录用来保存某项目相关文件。

选项-p 同时创建目录和它的子目录。

```
mkdir -p 目录名/子目录名
```

（4）删除目录

当目录不再被使用，或者磁盘空间已达到使用限定值，就需要从文件系统中删除失去使用价值的目录。利用 rmdir 命令从目录中删除一个或多个空的子目录，语法格式如下：

```
rmdir [选项] 目录名[目录名…]
```

子目录被删除之前应该是空目录。就是说，该目录中的所有文件必须已清空。如果该目录中仍有其他文件，那么就不能用 rmdir 命令把它删除。

当前的工作目录必须在被删除目录之上，不能是被删除目录本身，也不能是被删除目录的子目录。

① -p：递归地删除指定的目录及其子目录。即：如果指定的目录有子目录，就先删除其子目录，然后删除该目录。

② -r：递归地删除目录中的所有文件和该目录本身。

（5）显示当前目录

在具体操作时，很多时候可能会记不清用户当前所在的目录，命令 pwd 可以显示用户当前在目录树中的位置。如：

```
# pwd
# /usr/local/rfinput/bin
```

系统给出的信息表示用户当前所在的目录是/usr/local/rfinput/bin。

4）文件操作命令

（1）显示文本文件

文本文件是由可打印字符和控制字符（如制表符和换行符）组成的。有几个命令可以显示文本文件。

① cat 命令，其语法如下：

```
cat[选项] 文件名[文件名…]
```

该命令运行后，指定文件的内容就在标准输出（通常是屏幕）上显示出来。如果文件的内容很长，在一个屏幕中显示不下，就会出现屏幕滚动，为了控制滚屏，可以按 Ctrl＋S 键，停止滚屏；按 Ctrl＋Q 键可以恢复滚屏。其中选项及其意义如下：

- -v：用一种特殊形式显示控制字符，除去 LFO 与 TAB。

- -n：显示输出行的编号。
- -b：显示非空输出行的编号。

② head 命令，其语法如下：

```
head [显示行数] 文件名[文件名…]
```

head 命令在屏幕上显示指定文件最前面的若干行，行数由“显示行数”确定，默认值是 10。

③ tail 命令，其语法如下：

```
tail [显示行数] 文件名[文件名…]
tail [+n] 文件名[文件名…]
```

在屏幕上显示指定文件末尾的若干行，行数由“显示行数”确定；或者从指定行号开始显示，直至该文件的末尾。

④ more 命令，显示文件内容，每次显示一屏，其语法是：

```
more [选项] 文件名[文件名]
```

可在每个屏幕的底部出现一个提示信息，给出至今已显示的该文件的百分比。

可以用几种不同的方法对提示作出回答：

- 按 Space 键，显示文本的下一屏内容。
- 按 Enter 键，只显示文本的下一行内容。
- 按斜线符(/)，接着输入一个模式，可以在文本中寻找下一个相匹配的模式。
- 按 h 键，显示帮助屏，该屏上有相关的帮助信息。
- 按 b 键，显示上一屏内容。
- 按 q 键，退出 more 命令。

(2) 创建新文件

可以利用命令和实用程序来创建文件，如文本编辑器，专门用于把有用的数据放入文件中。然而，有时可能只需要仅有文件名的文件，即空文件。Linux 系统提供 touch 命令来创建空文件。其语法如下：

```
touch 文件名[文件名…]
```

不存在的文件名被当作空文件创建。已存在文件的时间标签会更新为当前的时间（默认方式），它们的数据将原封不动地保留下来。

(3) 复制文件

使用 cp 命令可以做文件的备份，或者做其他用户文件的复制。可以使用 cp 命令把一个源文件复制到一个目标文件，或者把一系列文件复制到一个目标目录中。其语法是：

```
cp 源文件 目标文件
cp 源文件 1 [源文件 2…] 目标文件
```

在第一种语法格式中，源文件被复制到目标文件。如果目标文件是目录文件，那么把源文件复制到这个目录中，而文件名保持不变；如果目标文件不是目录文件，那么源文件就复制到该目标文件中，后者原有的内容将被破坏，但文件名不变。

在第二种语法格式中，所有的源文件都被复制到目标文件，该目标文件必须是目录文件，所有源文件的名字都不变。

(4) 移动和重命名文件

mv 命令用来移动文件或对文件重命名，其语法为：

```
mv 源文件目标文件
mv 源文件 1 [源文件 2…] 目标文件
```

在第一种语法中，源文件被移至目标文件后有两种不同的结果：如果目标文件是某一目录文件的路径，源文件会被移到此目录下，且文件名不变；如果目标文件不是目录文件，则源文件名会变为此目标文件名，并覆盖已存在的同名文件。

在第二种语法中，所有的源文件都会被移至目标文件，这里的目标文件必须是目录文件。所有移到该目录下的文件都将保留以前的文件名。

如果将一个文件移到一个已经存在的目标文件，则目标文件的内容将被覆盖。

如果源文件和目标文件在同一个目录下，mv 的作用就是重命名文件，例如：

```
mv oldname newname
```

(5) 删除文件

用 rm 命令删除不需要的文件和目录，其语法为：

```
rm [选项] 文件名 1 [文件名 2…]
```

在删除文件之前，最好再看一下文件的内容，确定是否真正要删除。

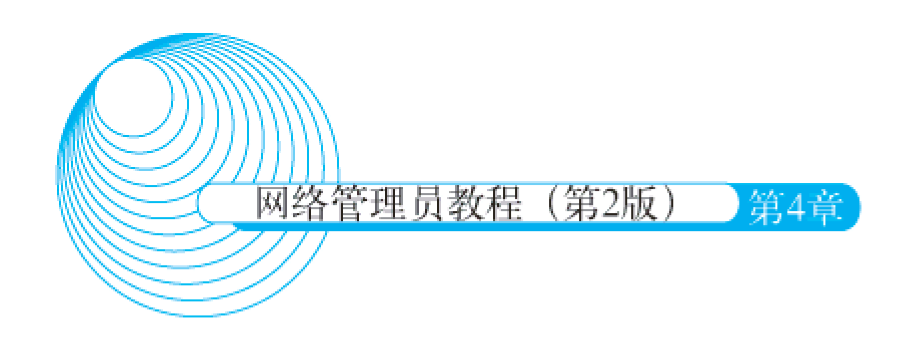
① -i：这个选项在使用文件扩展名字符删除多个文件时特别有用。此选项会要求用户逐一确定是否要删除文件，必须输入 y 或 Y，按 Enter 键后才能删除文件。如果仅按 Enter 键或其他字符键，文件不会被删除。

② -r：可以删除目录。当一个目录被删除时，该目录下所有文件和子目录都将被删除。

(6) 文件链接

红旗 Linux 具有为一个文件起多个名字的功能，称为链接。这样只要对一个文件进行修改，就可以完成对所有目录下相应链接文件的修改。

ln 命令用来创建链接，其语法为：



ln 源文件目标文件

ln 源文件 1 [源文件 2…] 目标文件

在第一种语法格式中，如果目标文件是到某一目录文件的路径，源文件会链接到此目录下，文件名不变；如果目标文件不是到某一目录文件的路径，源文件会链接到此目标文件，并覆盖已经存在的同名文件。

在第二种语法格式中，所有的源文件都被链接到目标文件——该目标文件必须是目录文件。所有源文件的名字都不变。

文件链接有两种形式，即硬链接和符号链接。

① 硬链接，默认情况下用 ln 命令创建硬链接。一个文件的硬链接数可以在目录的长列表格式的第二列中看到，无额外链接的文件链接数为 1。ln 命令会增加链接数，rm 命令会减少链接数。一个文件除非链接数为 0，否则不会物理地从文件系统中被删除。

对硬链接有如下限制：不能对目录文件作硬链接；不能在不同的文件系统之间作硬链接。

② 符号链接，也称软链接，是将一个路径名链接到一个文件，事实上，它只是一个文本文件，其中包含它提供链接的另一个文件的路径名。另一个文件是实际包含所有数据的文件。所有读写文件内容的命令，当它们被用于符号链接时，将沿着链接方向前进去访问实际的文件。

如果给 ln 命令加上 s 选项，则建立符号链接。例如：

ln -s source destination

符号链接没有硬链接的限制，可以对目录文件作符号链接，也可以在不同文件系统之间作符号链接。

(7) 文件内容比较

① 比较文本文件：diff 命令用于比较文本文件，并显示两个文件的不同。如两个文件完全一样，则不显示任何输出。如有区别，就会分段显示两个文件的区别。其一般格式是：

diff 文件 1 文件 2…

② 比较数据文件：cmp 命令比较任何两个包含正文或数据的普通文件。由于二进制数据不能显示到屏幕上，cmp 命令只是简单的报告从哪一个字节开始出现不同。其一般语法为：

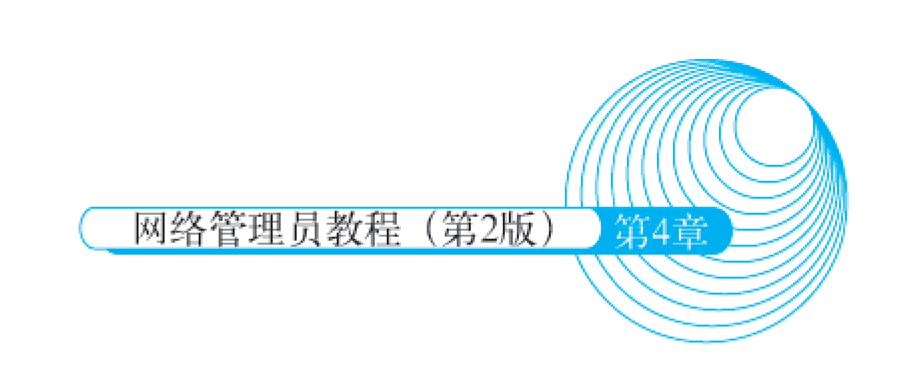
cmp file1 file2

(8) 查找文件

① find 命令：用来查找文件和目录的位置。该命令的语法为：

find 路径名[选项]

其中，常用的选项介绍如下。



-print：显示输出查找到的结果。如果未指定任何选项，则系统默认是-print。如 find 命令的最基本的用法就是列出指定目录下的所有文件和子目录。

```
# find /usr -print
```

-name：按文件名查找。

-size：按文件大小查找。

例如，下面的命令将查找/usr 目录下超过 100KB 的文件。

```
# find /usr -size 100k
```

-user：按文件主查找。

-type：按文件类型查找。常见的类型有：

- b——块特别文件；
- c——字符特别文件；
- f——普通文件；
- l——符号链接文件；
- d——目录文件。

② locate 命令：一个使用方便且查询速度极快的文件和目录查找命令。该命令的语法为：

```
locate 文件名[选项]
```

使用 locate 命令的前提是要先创建一个用于定位文件或目录位置的 slocate 数据库，而且该数据库应是时时更新的，这样才可以保证 locate 查找结果的准确性。以下命令用于从 / 开始创建 slocate 数据库：

```
# locate -u
```

数据库创建后就可以查找文件了。例如，要查找所有关于 telnet 命令的文件，可以使用：

```
# locate telnet
```

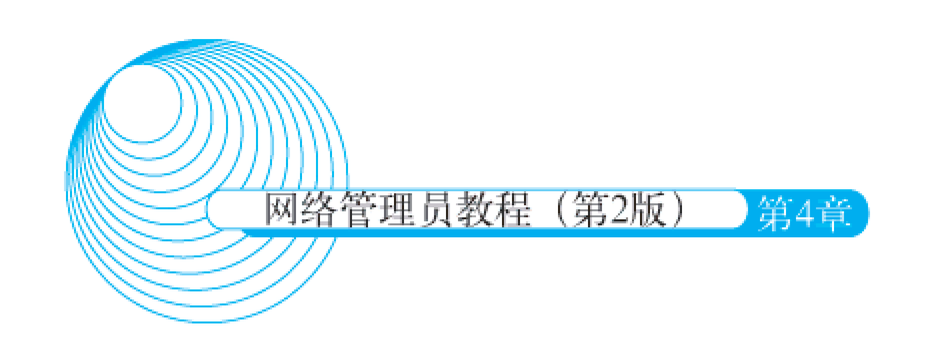
locate 命令将在其数据库中检查所有匹配于 telnet 的文件和目录并在屏幕上显示结果。更新 slocate 数据库的命令是 updatedb，需要以 root 用户身份执行此命令。

一般情况下，系统管理员会设置由 cron 程序在夜间自动更新数据库。cron 是一个后台守护进程，它定期执行计划好的任务。

(9) 在文件中查找正文

grep 命令用来在文本文件中查找指定模式的词或短语，并在标准输出上显示包括给定字符串的所有行。grep 命令的语法为：

```
grep [选项] 查找模式文件名[文件名…]
```



默认情况下，grep 在查找模式时是区分大小写的；如不想区别大小写，可以用选项-i。

例如，下面的命令将在/etc 目录及其子目录下的所有文件中查找字符串“hello world”出现的次数：

```
# grep 'hello world' /etc/ * / *
```

查找模式可能是唯一的参数，如果在模式中使用了 shell 元字符，通常要使单引号(')把它括起来。

5）文件权限操作

在多用户操作系统中，出于安全性的考虑，需要给每个文件和目录加上访问权限，严格地规定每个用户的权限。同时，用户可以为文件赋予适当的权限，以保证他人不能修改和访问。

（1）改变文件属主

Linux 为每个文件都分配了一个文件所有者，称为文件属主，对文件的控制取决于文件主或超级用户(root)。文件或目录的创建者对创建的文件或目录拥有特别使用权。文件的所有关系是可以改变的，chown 命令用来更改某个文件或目录的所有权。chown 命令的语法格式是：

```
chown [选项] 用户或组文件 1 [文件 2…]
```

用户可以是用户名或用户 ID。文件是以空格分开的要改变权限的文件列表，可以用通配符表示文件名。

如果改变了文件或目录的所有权，原文件属主将不再拥有该文件或目录的权限。系统管理员经常使用 chown 命令，在将文件复制到另一个用户的目录下以后，让用户拥有使用该文件的权限。

（2）改变用户组

在 Linux 下，每个文件又同时属于一个用户组。当创建一个文件或目录，系统就会赋予它一个用户组关系，用户组的所有成员都可以使用此文件或目录。

文件用户组关系的标志是 GID。文件的 GID 只能由文件主或超级用户(root)来修改。chgrp 命令可以改变文件的 GID，其语法格式为：

```
chgrp [选项] group 文件名
```

其中 group 是用户组 ID。文件名是以空格分开的要改变属组的文件列表，它支持通配符。

（3）文件权限设置

Linux 系统中的每个文件和目录都有访问许可权限，用它来确定谁可以通过何种方式对文件和目录进行访问和操作。访问权限规定 3 种不同类型的用户：文件属主(owner)、同组用户(group)、可以访问系统的其他用户(others)。

访问权限规定 3 种访问文件或目录的方式：读(r)、写(w)、可执行或查找(x)。

当用 ls -l 命令或 l 命令显示文件或目录的详细信息时，最左边的一列为文件的访问权限，其中各位的含义如图 4-92 所示。

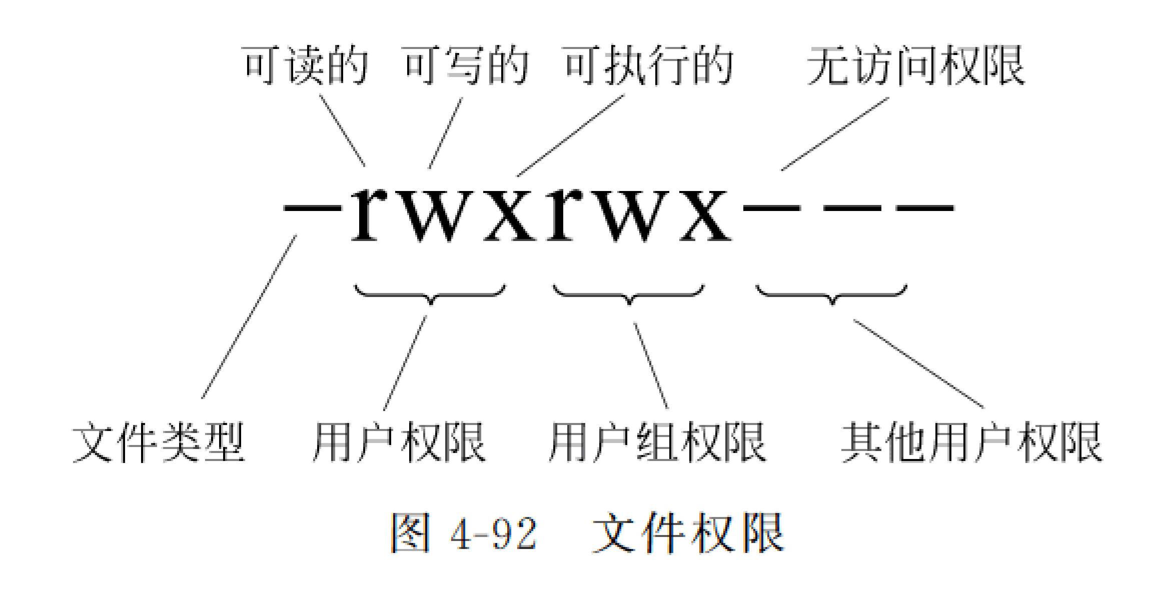


图 4-92 文件权限

① 对于文件而言：

- 读权限(r)只允许指定用户读其内容，而禁止对其做任何的更改操作。将所访问的文件的内容作为输入的命令都需要有读的权限，如 cat、more 等。
- 写权限(w)允许指定用户打开并修改文件，如命令 vi、cp 等。
- 执行权限(x)指定用户将该文件作为一个程序执行。

② 对于目录而言：

- 读权限(r)可以列出存储在该目录下的文件，即读目录内容列表。这一权限允许 shell 使用文件扩展名字符列出相匹配的文件名。
- 写权限(w)允许从目录中删除或添加新的文件，通常只有目录主才有写权限。
- 执行权限(x)允许在目录中查找，并能用 cd 命令将工作目录改到该目录。

(4) 改变文件权限

chmod 用于改变文件或目录的访问权限。用户可以用它控制文件或目录的访问权限。只有文件主或超级用户 root 才有权用 chmod 改变文件或目录的访问权限。chmod 命令的语法为：

chmod key 文件名

key 由以下各项组成：

[who] [操作符号] [mode]

这 3 部分必须按顺序输入。可以用多个 key，但必须以逗号间隔。

① 操作对象 who 可以是下述字母中的任一个或者它们的组合：

- u(user)，表示用户，即文件或目录的所有者。
- g(group)，表示同组用户，即与文件属主有相同组 ID 的所有用户。
- o(others)，表示其他用户。
- a(all)，表示所有用户，它是系统默认值。

② 操作符号可以是：

- ＋，添加某个权限。
- －，取消某个权限。
- ＝，赋予给定权限并取消其他所有权限(如果有的话)。

③ mode 所表示的权限可用下述字母的任意组合：

- r，可读。
- w，可写。
- x，可执行。
- s，在文件执行时把进程的属主或组 ID 置为该文件的文件属主。
- t，保存程序的文本到交换设备上。
- u，与文件属主拥有一样的权限。
- g，与和文件属主同组的用户拥有一样的权限。
- o，与其他用户拥有一样的权限。

通常也可以用 chmod 命令配以不同类型的 key 直接设置权限。这时以数字代表不同的权限。key 是以 3 位八进制数字出现的，第 1 位表示用户权限，第 2 位表示组权限，第 3 位表示其他用户权限。数字表示的属性的含义为：0 表示禁止该权限，1 表示可执行权限，2 表示可写权限，4 表示可读权限，然后将其相加。所以数字属性的格式应为 3 个从 0 到 7 的八进制数，其顺序是(u)、(g)、(o)。

例如，要使文件 myfile 的文件主和同组用户具有读写权限，但其他用户只可读，可以用以下命令指定权限：

```
chmod 664 myfile
```

(5) 默认权限

默认情况下，系统将创建的普通文件的权限设置为-rw-r-r-- ，即文件主对该文件可读可写(rw)，而同组用户和其他用户都只可读；同样，在默认配置中，将每一个用户主目录的权限都设置为 drwx------ ，即只有文件主对该目录可读、写和可查询(rwx)，即用户不能读其他用户目录中的内容。用户可以修改新建文件的默认存取权限，如使用如下命令：

```
umask u=rwx,g=,o=
```

它会在创建新文件时给文件主以全部权限，而同组用户及其他用户没有任何权限。

6) 进程和作业控制命令

简单地说，进程是一个程序或任务的执行过程。在 Linux 系统中，执行任何一个命令都会创建一个或多个进程。就是说，命令是通过进程实现的。从进程的角度可以更好地理解 Linux 操作系统的多任务概念。对于系统管理员来说，管理系统进程是日常管理的重要部分。

(1) ps 命令

可以通过 ps 命令观察进程状态，它会把当前瞬间进程的状态显示出来。可以根据显示的信息确定哪个进程正在运行，某个进程是被挂起，还是遇到了某些困难，进程已运行了多久，进程正在使用的资源，进程的相对优先级，以及进程的标识号（PID）。所有这些信息对用户都很有用，对于系统管理员来说更为重要。

ps 命令的一般用法是：

```
ps [option [arguments]…
```

ps 命令有以下几个主要的参数。

- -a：显示包括系统中所有用户进程的状态。
- -f：显示进程和子进程的树型目录。
- -l：以长列表形式显示进程信息。
- -r：只显示正在运行的进程。
- -u：以用户格式显示进程信息，给出用户名和起始时间。
- pids：显示指定 ID 的进程的信息。

如果不带任何选项，ps 命令列出每个与当前 shell 有关的进程的 PID。结果如下：

```
PID     TTY      TIME       CMD
596     pts/0    00:00:00   bash
627     pts/0    00:00:00   vi
628     pts/0    00:00:00   ps
```

其中，各字段的含义如下。

- PID：进程标识号。
- TTY：开始该进程的终端号。
- TIME：报告进程累计使用的 CPU 时间。
- CMD：正在执行的进程名。

要获得一个完整的进程信息列表，可以使用带有下列选项的 ps 命令：

```
ps - aux
```

它除了列出以上字段以外，还列出 CPU 使用率（%CPU）、内存使用率（%MEM）、虚拟映像大小（SIZE）、驻留数据集大小（RSS）、终端号（TTY）、状态（STAT）。

（2）top 命令

top 命令用于读入计算机系统的信息，这些信息包括当前的系统数据和进程的状态等。输入 top 命令后，屏幕的输出包括以下几个部分。

① Uptime：显示当前时间、自上次启动系统开始过去的时间、激活用户的数目以及在过去 1、5 和 15 分钟之内的 CPU 平均占用情况。

② Process：显示了系统所有的进程，并把进程按挂起、运行、创建和停止分类。

③ CPU states：统计被用户和系统占用的当前 CPU 的状态。

④ Mem：统计当前内存的占用状态。

⑤ Swap：统计 swap 区域的占用情况。

在 top 命令中显示了进程的列表，其中包括的内容有：PID、用户、优先级、nice 参数、所需的内存信息(SIZE、RSS、SHARE)、状态(STAT)、CPU 占用的百分比、占用的内存信息、已用的计算机时间和各自的程序调用(COMMAND)等。关于 top 命令的详细使用信息，可查看其在线帮助。

(3) kill 命令

运行过程中，可能在某一时刻，系统中有的进程出现了问题，不能正常运行，但也不能正常退出。这时可以使用 kill 命令终止进程的执行，释放这些进程占用的系统资源，常用的 kill 命令的语法格式为：

```
kill [-s signal] pid
kill  - l [signal]
```

命令的选项和参数的意义如下：

① pid 给出了需要结束的进程的 PID，可以通过命令 ps 获得进程的 PID。在命令 kill 中可以一次列出许多的进程 PID。

② -s signal 是一个可选参数，用来给出发给进程的信号。在默认情况下，命令 kill 给进程发 TERM 信号，该信号将通知进程退出。如果进程不接收该信号，可以通过参数-9 强行结束进程。

③ -l 参数要求 kill 命令列出它可以发给进程的所有信号。

(4) at 命令

at 命令实现在指定的时间运行安排的作业。at 命令的一般用法如下：

```
at [选项] 时间[日期]
```

① at hh:mm：用指定的小时(hh)和分钟(mm)(24 小时制)安排作业。

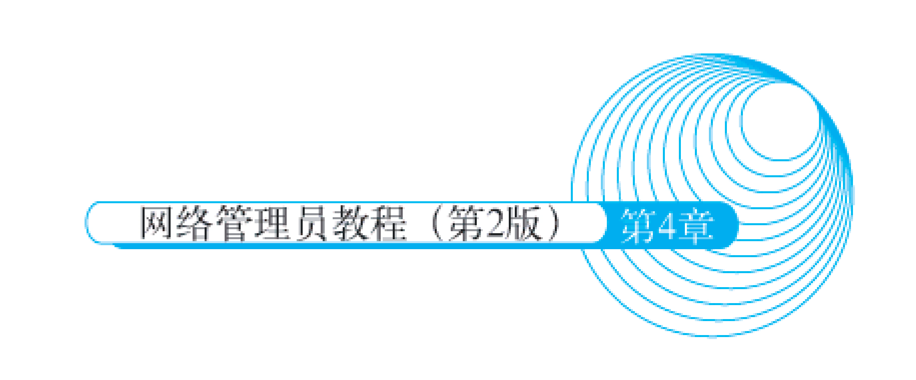
② at hh:mm month day year：用指定的年(year)、月(month)、日(day)、小时(hh)和分钟(mm)安排作业。

③ at - l：列出已安排的作业。

④ at now +count time_units：作业运行的时间安排在现在的时间加上 count 个时间单位，时间单位(time_units)可以是分钟、小时、天或星期。

⑤ at - d job_id：取消作业号与 job_id 相同的作业。

由 at 命令调度的命令是在 at 命令行后输入的命令列表。at 的命令列表可以从标准输入(stdin)得到。如果标准输入来自键盘，应在输入完命令之后按 Ctrl+D 键，表明输入结束。



7）基本网络命令

Red Flag Server 4.0 具有强大的网络功能，提供了丰富的网络应用程序，完全支持 TCP/IP 协议。在网络环境下，可以进行远程注册、远程命令调用、传送文件等操作。

（1）telnet 命令

telnet 命令是 Linux 下的远程登录工具，只要拥有合法的注册名和口令，就能像使用本地机器一样访问远程计算机了。telnet 也允许用户通过输入注册名和口令从远程网点登录到自己的计算机上，从而通过网络或电话线完成检查电子邮件、编辑文件和运行程序等操作。但是 telnet 只能在字符终端方式下工作，不支持图形用户界面。telnet 的基本用法是：

```
telnet [选项] IP 地址/主机名
```

命令输入后，telnet 即会启动一个远程会话，本命令可使用的主要选项参数说明如下。

① -d：启动调试功能。

② -a：自动注册。

③ -n tracefile：打开跟踪程序，把跟踪程序数据保存在 tracefile 中。

④ -e escape_char：将会话的转义字符设置为 escape_char。

⑤ -l user：把用户名发送给远程系统，以便自动注册。本参数自动包括-a 参数。

⑥ port：指出与远程系统连接的端口号，如不指定，将连接到默认端口。

成功地连接到远程计算机上后，telnet 就显示登录信息，并提示用户输入注册名与口令，如注册成功，就可以开始工作了。

在使用 telnet 后需要退出注册回到本地的 shell 命令提示符下。

（2）ping 命令

ping 命令用来确定网络上的主机是否可到达和到达速率。该命令的语法格式为：

```
ping [选项] IP 地址/主机名
```

ping 命令将大小固定的数据包发送给对方，并要求对方返回。当终止 ping 命令时，会显示一些统计数据。通过数据判断是否返回以及返回时间，用户可以确定对方是否可到达，是否开机，以及网络延时时间。如果要退出，按 Ctrl+C 键中断。

（3）finger 命令

使用 finger 命令来查询系统用户的信息，该命令的基本格式为：

```
finger [选项] 用户名@主机名
```

运行 finger 命令后会显示系统中某个用户的用户名、主目录、停滞时间、登录时间、登录 shell 等信息，查询远程机上的用户信息时，需要在用户名后面加上“@主机名”的方式。

第5章　应用服务器配置

5.1　DNS 服务器配置

5.1.1　DNS 服务器基础

域名系统(DNS)是一种 TCP/IP 的标准服务，负责 IP 地址和域名之间的转换。DNS 服务允许网络上的客户机注册和解析 DNS 域名。这些名称用于为搜索和访问网络上的计算机提供定位。

域名服务器负责控制本地数据库中的名字解析。DNS 的数据库结构形成一个倒立的树状结构，树的每一个节点都表示整个分布式数据库中的一个分区(域)，每个域可再进一步划分成子分区(域)。每个节点有一个至多达 63 个字符长的标识，命名标识中一律不区分大小写。节点的域名是从根到当前域所经过的所有节点的标记名，从右到左排列，并用点“.”分隔。域名树上的每一个节点必须有唯一的域名。每个域名对应一个 IP 地址，一个 IP 地址可以对应多个域名。

一个域名服务器可以管理一个域，也可以管理多个域，通常在一个域中可能有多个域名服务器，域名服务器有以下几种类型。

(1) 主域名服务器(Primary Name Server)：负责维护这个区域的所有域名信息，是特定域所有信息的权威性信息源。一个域有且只有一个主域名服务器。它从域管理员构造的本地磁盘文件中加载域信息，该文件(区文件)包含着该服务器具有管理权的一部分域结构的最精确信息。主服务器是一种权威性服务器，因为它以绝对的权威去回答对本域的任何查询。

(2) 辅域名服务器(Secondary Name Server)：当主域名服务器关闭、出现故障或负载过重时，辅域名服务器作为备份服务器提供域名解析服务。辅助服务器从主域名服务器获得授权，并定期向主服务器询问是否有新数据，如果有则调入并更新域名解析数据，以达到与主域名服务器同步的目的。在辅助域名服务器中有一个所有域信息的完整备份，可以权威地回答对该域的查询，因此，辅助域名服务器也称作权威性服务器。

(3) 缓存域名服务器(Caching-Only Server)：可运行域名服务器软件但是没有域名数据库。它从某个远程服务器取得每次域名服务器查询的回答，一旦取得一个答案，就将它放在高速缓存中，以后查询相同的信息时就用它予以回答。缓存域名服务器不是权威性服务器，因为它提供的所有信息都是间接信息。

(4) 转发域名服务器(Forwarding Server)：负责所有非本地域名的本地查询。转发域名服务器接到查询请求时，在其缓存中查找，如找不到就把请求依次转发到指定的域名服务器，直到

查询到结果为止，否则返回无法映射的结果。

另外，还需要了解两个概念：一个是正向解析，表示将域名转换为 IP 地址；另一个是反向解析，表示将 IP 地址转换为域名，反向解析时要用到反向域名，顶级反向域名为 in-addr. arpa.，例如一个 IP 地址为 200. 20. 100. 10 的主机，它所在域的反向域名是 100. 20. 200. in-addr. arpa。

需要说明的是 Windows server 2003 也提供了 DNS 服务器角色，使用图形化的方式可以很方便地配置 DNS 服务器，因篇幅限制，本节不做讲解。本节主要以使用 Red Flag Server 4. 0 中的图形化 DNS 配置工具 rfdns 为例，讲解 DNS 服务器配置的具体方法。

5.1.2 Red Flag Server 管理 DNS 服务器

1. 打开 DNS 配置工具

需要在 KDE 环境下以 root 权限运行 rfdns 配置工具。可以采用以下方法启动 DNS 配置工具。

(1) 在系统主菜单中选择“系统”→“控制面板”，打开控制面板，在“网络服务配置”标签页中，双击“DNS 配置工具”；

(2) 在系统主菜单中选择“管理工具”→“DNS 配置工具”；

(3) 在运行命令行或 shell 提示符下直接输入 rfdns。

2. 启动和停止 DNS 服务

打开 rfdns 配置工具，如图 5-1 所示。

在主窗口左侧的控制台树中，单击 DNS 服务器节点。

(1) 启动 DNS 服务，在菜单中选择“操作”→“所有任务”→“启动”；

(2) 停止 DNS 服务，在菜单中选择“操作”→“所有任务”→“停止”；

(3) 重新启动 DNS 服务，在菜单中选择“操作”→“所有任务”→“重新开始”。

操作结果将显示在主窗口右侧的消息窗口中。

管理员也可以在命令行终端下，通过下列命令执行大多数这些任务：

```
# /etc/init.d/named start
# /etc/init.d/named stop
# /etc/init.d/named restart
```

3. 指定转发域名服务器

转发域名服务器其他 DNS 服务器提供递归服务的 DNS 服务器。转发域名服务器一旦指定，即可用于帮助解析该服务器不能响应的任何 DNS 名称。

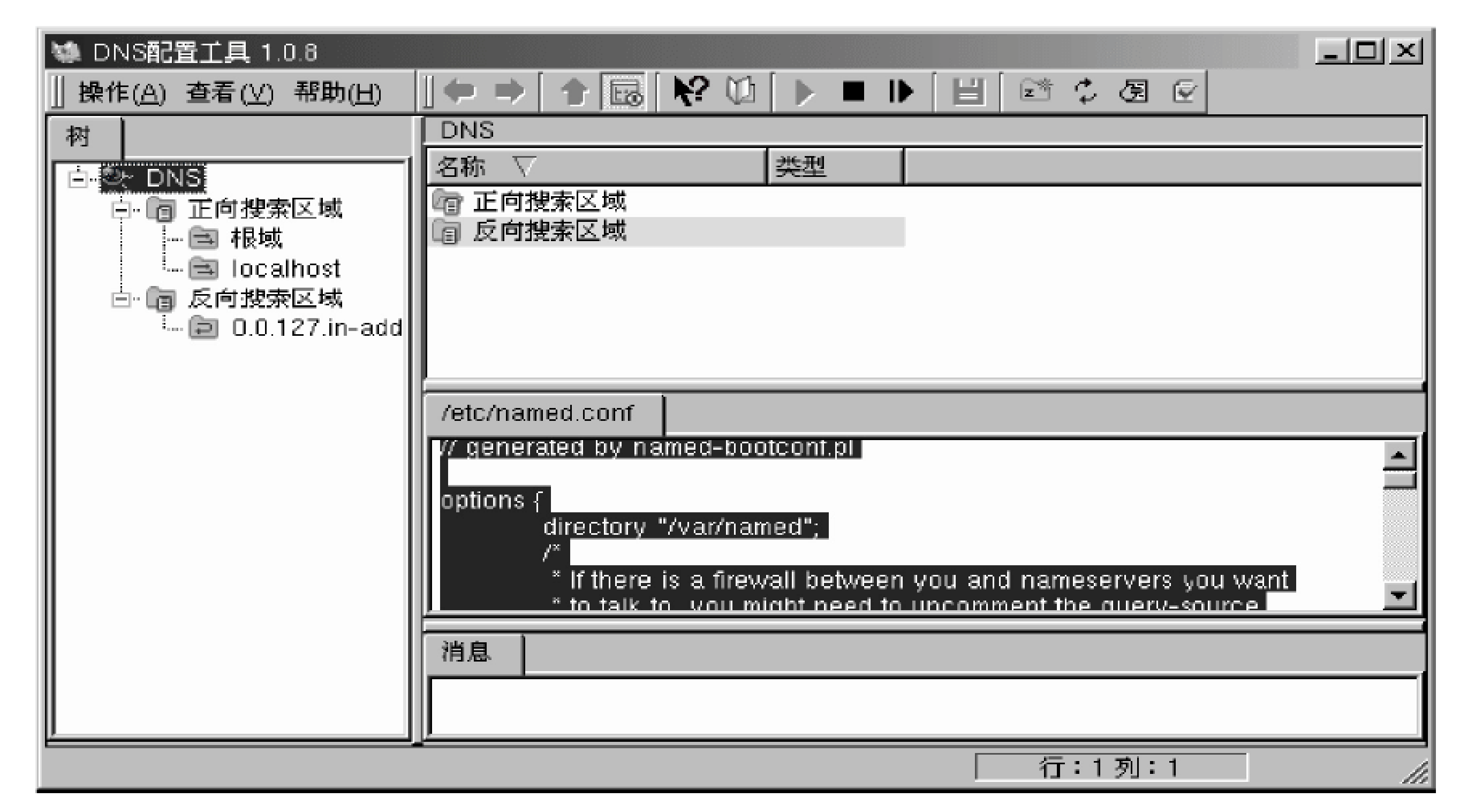


图 5-1　rfdns 主界面

打开 rfdns 配置工具，在主窗口左侧的控制台树中，单击“DNS”服务器节点。

选择菜单中的“操作”→“属性”，打开 DNS 服务器属性对话框，选中“启用转发器”后，添加可作为此服务器的转发器的其他 DNS 服务器的 IP 地址。

5.1.3　Red Flag Server 添加正向搜索区域

1．添加正向标准主要区域

(1) 在配置工具主窗口左侧的控制台树中，单击“正向搜索区域”。在菜单中选择“操作”→“新建区域”，弹出“新建区域向导”。单击“下一步”按钮继续，会出现图 5-2 所示的选择区域类型界面。开始要建立一个全新的区域，单击“标准主要区域”。

(2) 单击“下一步”按钮来确定新建区域的名称，如果申请的是一组域名，比如 redflag-linux.com，则只要输入到二级域；而不是连同子域或主机名称一起输入。如图 5-3 所示。

(3) 单击“下一步”按钮继续，如果要创建一个新的区域文件，就直接默认文件名，如图 5-4 所示。如果这个区域要使用从另一台计算机上复制的文件，则选中“使用此现存文件”。

(4) 选择区域文件后，单击“下一步”按钮，此时会出现以上步骤所设置的数据列表，如图 5-5 所示。如果一切设置正常，单击“完成”按钮将建立一个正向搜索区域，新建的区域将添加到主窗口的控制台树中。

2．添加正向标准辅助区域

(1) 添加正向标准辅助区域与添加正向标准主要区域的前面的步骤都相同，在图 5-2 所示

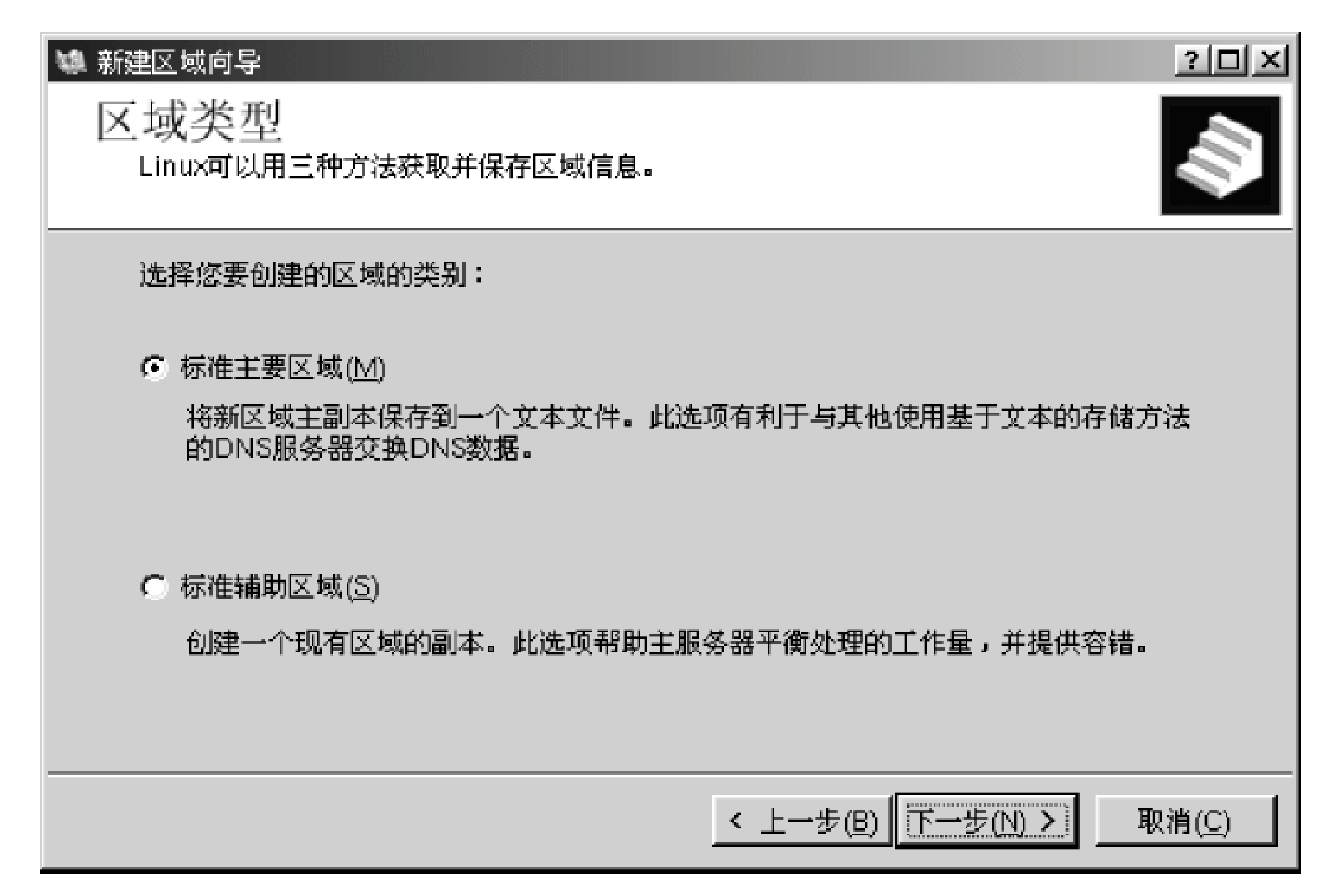


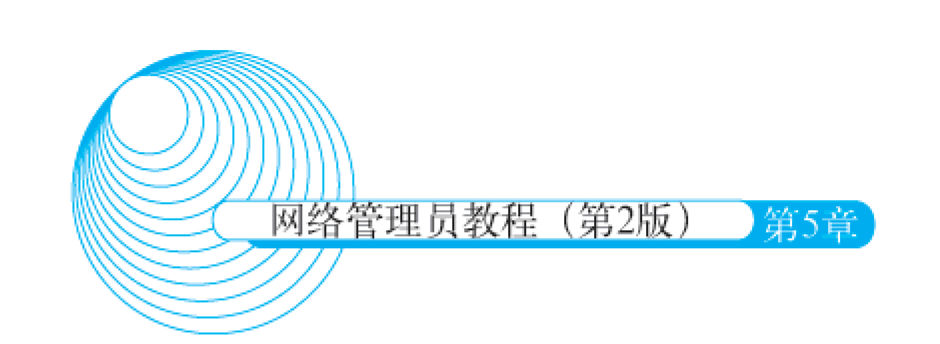
图 5-2　选择区域类型



图 5-3　设置区域名称

的区域类型选择界面中单击“标准辅助区域”。单击“下一步”按钮继续。在图 5-6 所示的界面中为新添的区域命名。

（2）单击“下一步”按钮进入图 5-7 所示的界面。此步骤用来设置想要复制区域的 DNS 服务器来源，可以一次复制多个服务器的数据。在“IP 地址”中输入可复制的服务器 IP 地址后，单击“添加”按钮；也可以在“服务器名”文本框中输入服务器的主机名后，单击“解析”按钮获得其 IP 地址再添加。接着单击“下一步”按钮，然后依向导提示完成设置。新建的区域将添加到主窗口的控制台树中。



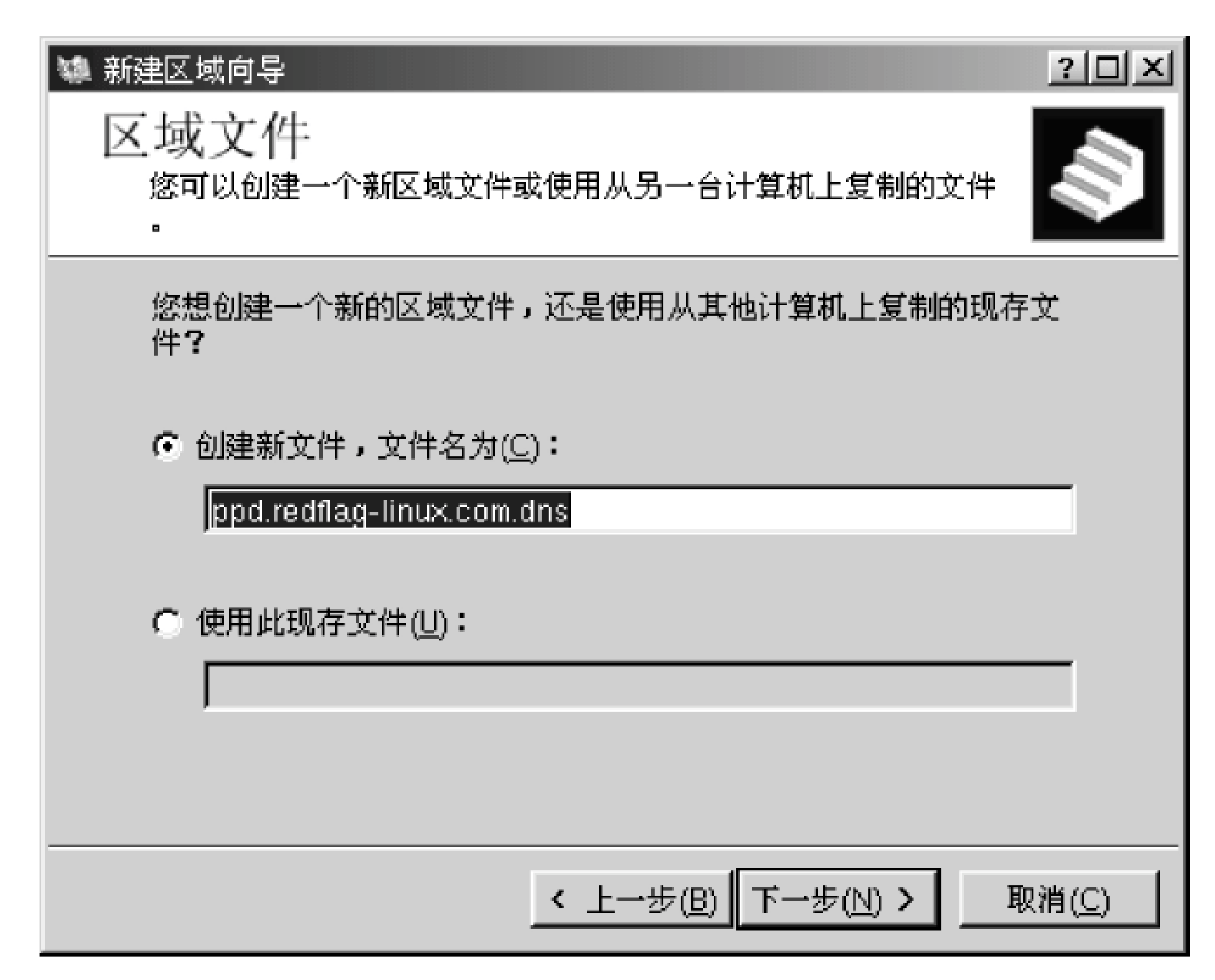


图 5-4　设置区域文件



图 5-5　完成正向标准主要区域

5.1.4　Red Flag Server 添加反向搜索区域

这里介绍添加反向标准主要区域的过程。



图 5-6　设置区域名称

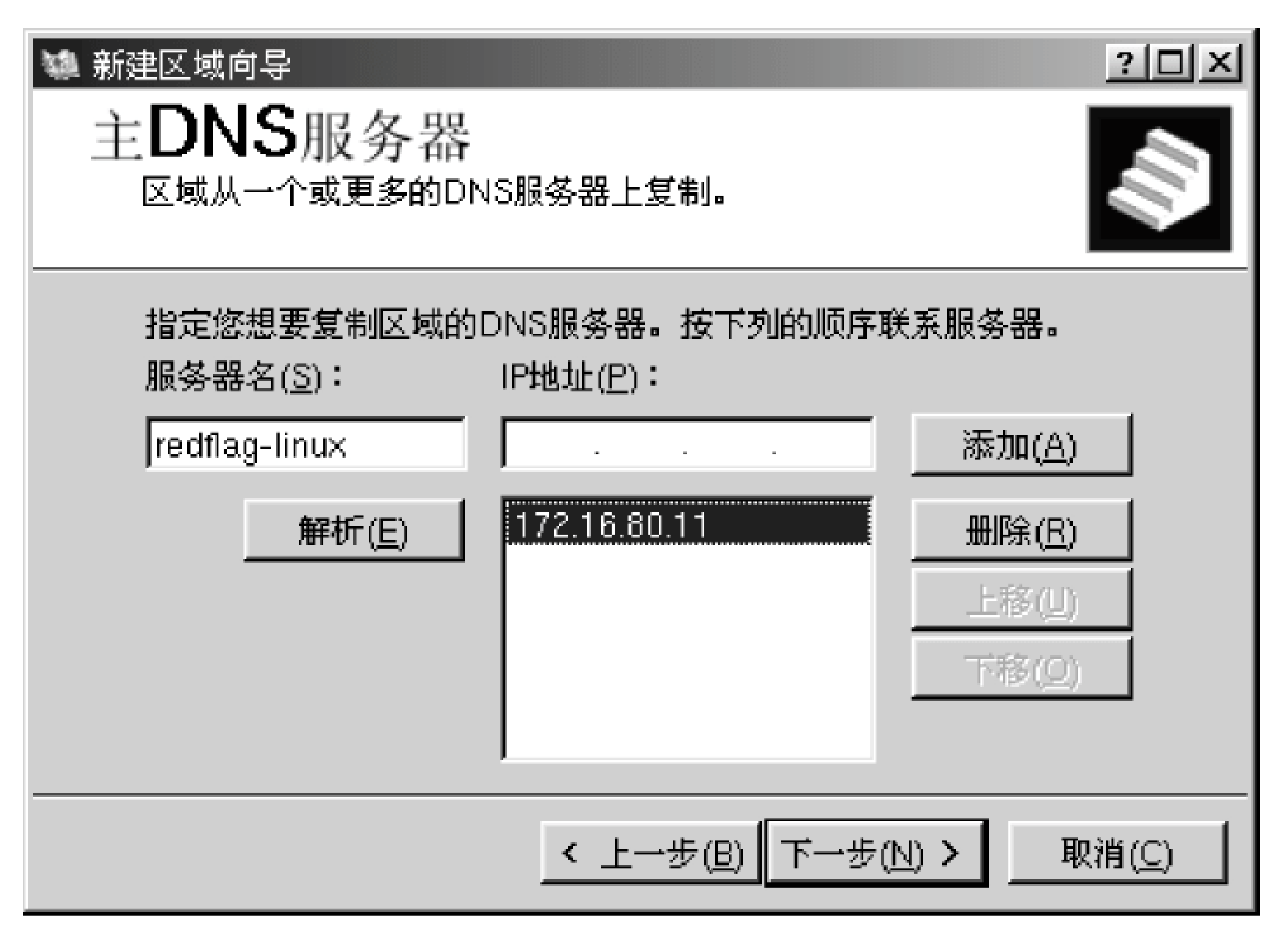


图 5-7　设置想要复制区域的服务器

(1) 在配置工具主窗口左侧的控制台树中，单击“反向搜索区域”。在菜单中选择“操作”→“新建区域”，弹出“新建区域向导”。

(2) 单击“下一步”按钮，会出现一个区域类型选择界面，单击“标准主要区域”。

(3) 单击“下一步”按钮，出现图 5-8 所示的界面。在“网络 ID”中，应该以 DNS 服务器 IP 地址的前 3 位来设置反向搜索区域。例如：所使用 DNS 服务器的 IP 地址是 172.16.82.11，则取其前 3 位即 172.16.82。然后，系统会在“反向搜索区域的名称”中，自动设置好 82.16.172.in-addr.arpa 的名称。

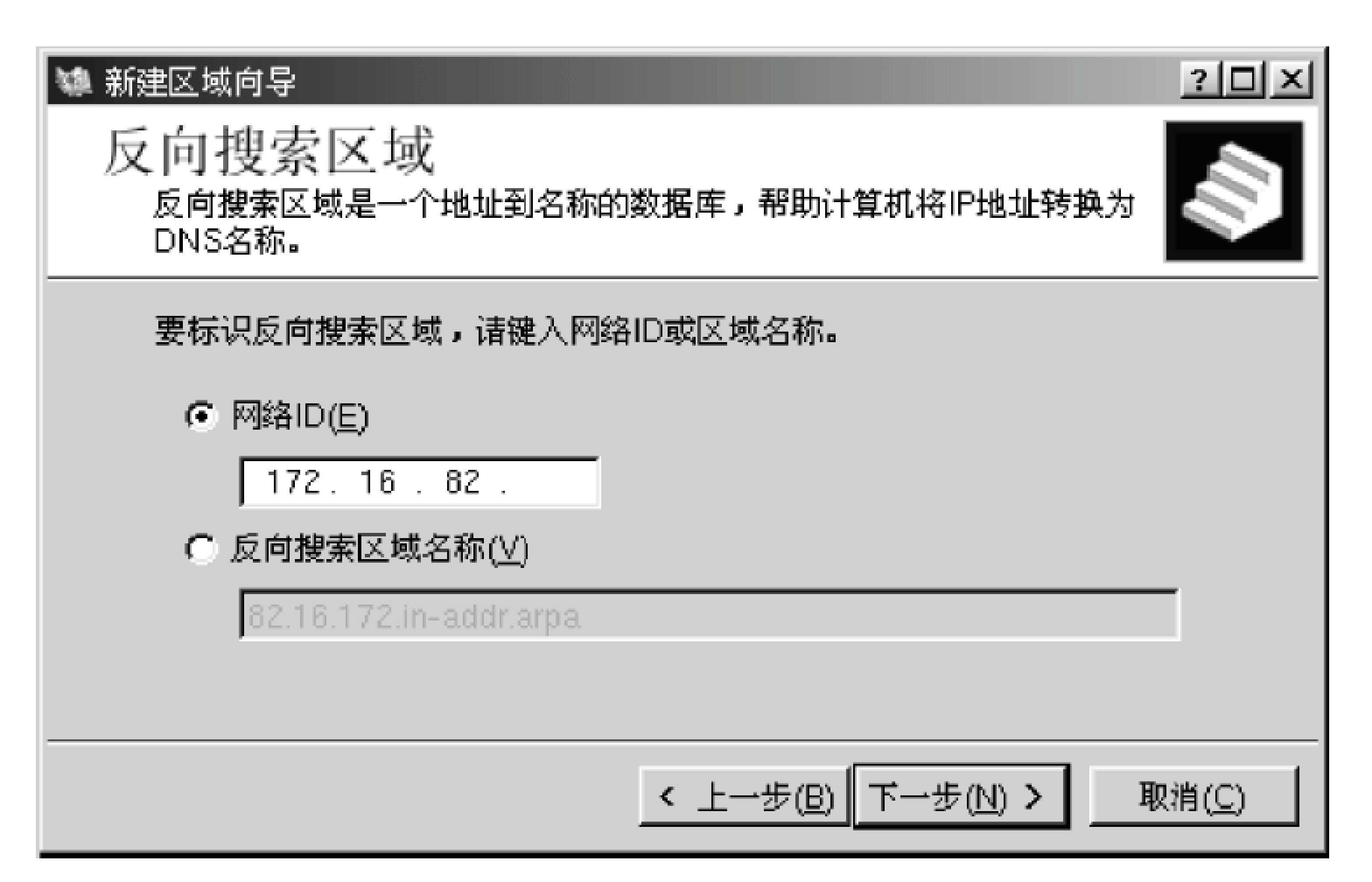


图 5-8 设置区域标识

（4）单击“下一步”按钮，出现设置区域文件的界面，直接使用默认的文件名即可，如图 5-9 所示。

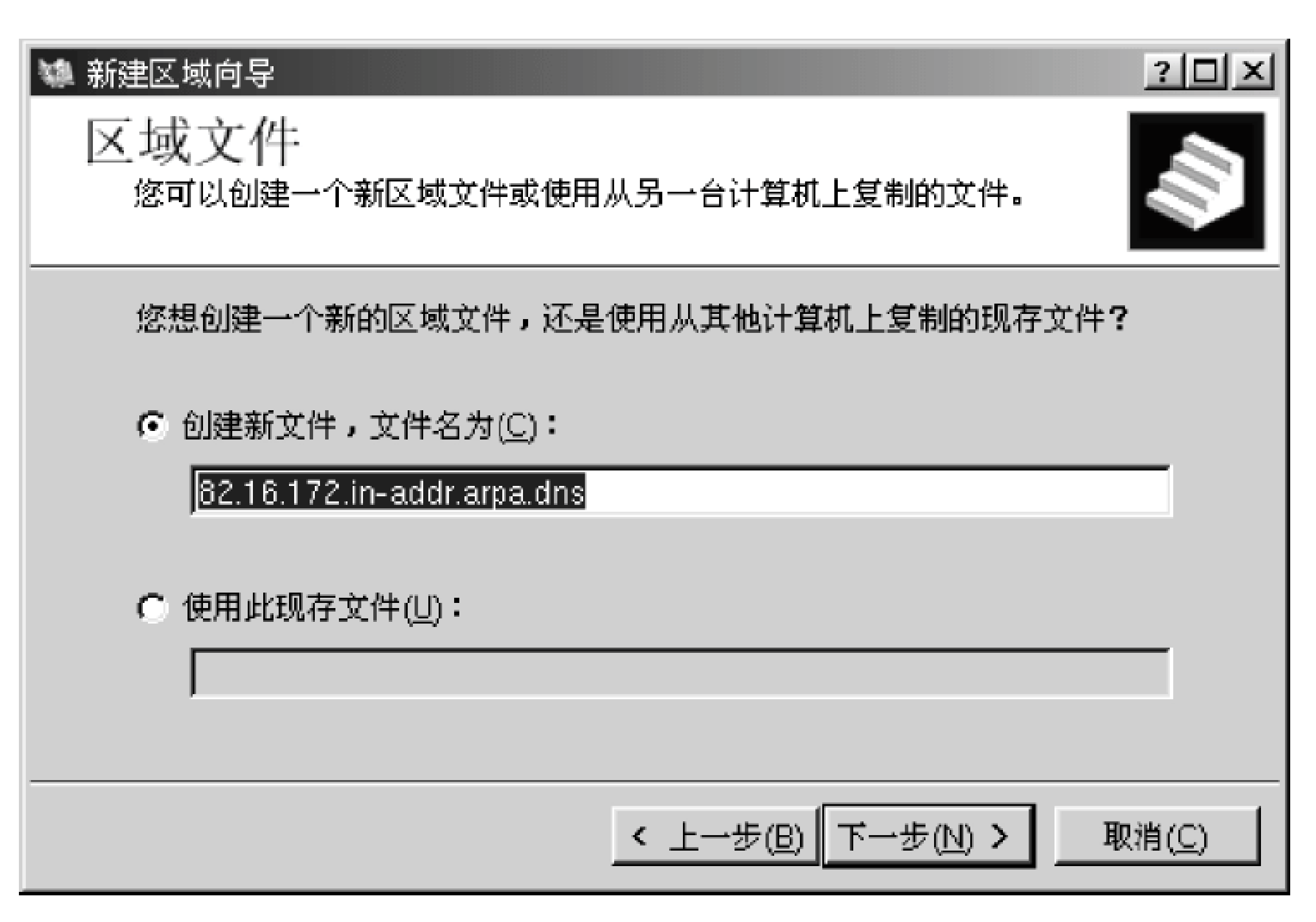


图 5-9 设置区域文件

（5）单击“下一步”按钮，此时会出现以上步骤所设置的数据列表。如果一切设置正常，单击“完成”按钮将建立一个反向搜索区域，新建的区域将添加到主窗口的控制台树中。

5.1.5 Red Flag Server 配置区域属性

1. 修改区域的起始授权机构(SOA)记录

SOA(Start of Authority)是用来识别域名中由哪一个命名服务器负责信息授权，在区域数据库文件中，第一笔记录必须是 SOA 的设置记录。

在配置工具主窗口左侧的控制台树中，选择相应的区域。单击菜单中的“操作”→“属性”，也可以右击选择快捷菜单中的“属性”菜单项。打开“区域属性”对话框，单击“起始授权机构(SOA)”配置页，如图 5-10 所示。

图 5-10 设置 SOA 记录

如有需要，可以修改“起始授权机构(SOA)”的属性。要调整“刷新间隔”、“重试间隔”或“过期间隔”，请在下拉列表中选择以秒、分钟、小时、天或星期为单位的时间段，然后在文本框中输入数字。单击“确定”按钮保存调整后的间隔。完成更改后单击“确定”按钮使修改生效。表 5-1 详细描述了设置界面中各选项的意义。

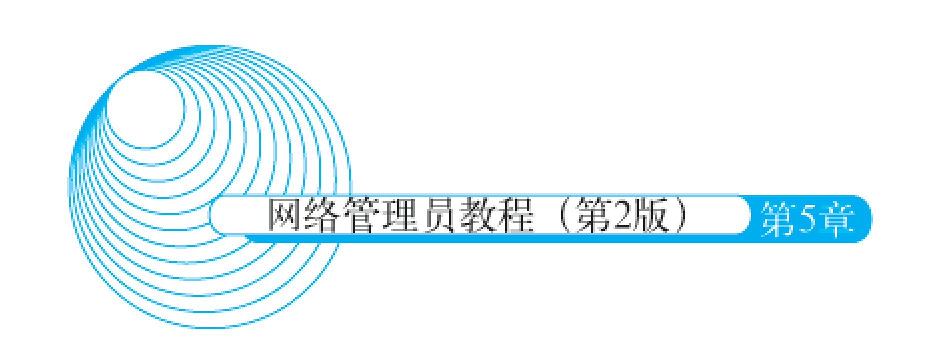


表 5-1　SOA 设置选项

设置选项	意义
序列号	当名称记录变动时，序列号也跟着增加，用以表示每次变动的序号，这样可以帮助辨认要进行动态更新的机器
主服务器	负责这个域的主要命名服务器
负责人	负责人名称后面有一个句点“.”，它表示 E-mail 地址中的@符号
刷新间隔	刷新间隔用于确定加载和维护此区域的其他 DNS 服务器必须尝试更新此区域的频率。默认情况下，每个区域的刷新间隔设置为 1 小时
重试间隔	重试间隔用于确定加载和维护此区域的其他 DNS 服务器在每次刷新间隔发生时重试区域更新请求的频率。默认情况下，每个区域的重试间隔设置为 10 分钟
过期间隔	过期间隔由配置为加载和维护此区域的其他 DNS 服务器使用，以决定区域数据在没有更新情况下何时过期。默认情况下，每个区域的过期间隔设置为 1 天
最小 TTL（默认）	每次域名缓存所停留在名称服务器上的时间
记录的 TTL	客户端查询名称，或其他名称服务器复制数据时，数据缓存在机器上的时间称为 TTL。默认的值为 1 小时

2．将其他 DNS 服务器指定为区域的权威服务器

在配置工具主窗口左侧的控制台树中，选择相应的区域。单击菜单中的“操作”→“属性”，也可以右击选择快捷菜单中的“属性”菜单项。打开“区域属性”对话框，单击“名称服务器”配置页，如图 5-11 所示。

如果要向列表中添加名称服务器，单击“添加”按钮，弹出“新建名称服务器”窗口，如图 5-12 所示。按 IP 地址指定其他的 DNS 服务器，然后单击“添加”按钮将它们加入列表。也可以通过输入其 DNS 名称将区域添加到权威服务器的列表中。输入名称时，单击“解析”按钮可以在将它添加到列表之前将其名称解析为 IP 地址。



图 5-11　设置名称服务器



图 5-12　添加名称服务器

使用该过程指定的 DNS 服务器将被加入到该区域现有的名称服务器(NS)资源记录中。

3. 为辅助区域更新主控服务器

在配置工具主窗口左侧的控制台树中，选择相应的辅助区域。单击菜单中的“操作”→“属性”，也可以右击选择快捷菜单中的“属性”菜单项。打开“区域属性”对话框。

单击“常规”配置页，在“IP 地址”中，为新的主控服务器指定 IP 地址并单击“添加”以便在列表中更新，如图 5-13 所示。



图 5-13　更新主控服务器

5.1.6　Red Flag Server 管理资源记录

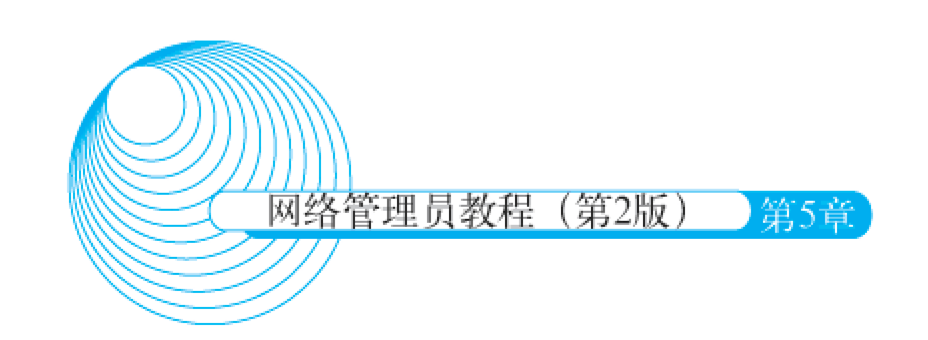
1. 向区域添加主机(A)资源记录

在配置工具主窗口左侧的控制台树中，选择相应的正向搜索区域。单击菜单中的“操作”→“新建主机”，也可以右击选择快捷菜单中的“新建主机”菜单项。打开如图 5-14 所示的 “新建主机”窗口。

在“名称”文本框中，填写新增主机记录的名称。不需要填上整个域名，比如要新增 sales 名称，只要输入 sales，而不是 sales. example. redflag-linux. com。

在“IP 地址”文本框中，输入新建主机的实际 IP 地址。

单击“添加主机”按钮，新增的主机记录将显示在主窗口右侧的列表中。重复上述动作可以向区域中添加多个主机资源记录。



2. 向区域添加别名(CNAME)资源记录

设置别名可以让一部主机拥有多个主机名称。例如，一部主机当作 Web 服务器时为 www.redflag-linux.com，而当作 FTP 服务器时可以是 ftp.redflag-linux.com。

在配置工具主窗口左侧的控制台树中，选择相应的正向搜索区域。单击菜单中的“操作”→“新建别名”，也可以右击选择快捷菜单中的“新建别名”菜单项。在“别名”文本框中，输入别名。在“目标主机的完全合格的名称”文本框中，输入使用此别名的 DNS 主机的完全合格域名。单击“确定”按钮，完成新增主机别名的动作，新增的主机别名将出现在主窗口右侧的列表中。



图 5-14　新建主机

3. 向区域添加邮件交换器(MX)资源记录

在配置工具主窗口左侧的控制台树中，选择相应的正向搜索区域。单击菜单中的“操作”→“新建邮件交换器”，也可以右击选择快捷菜单中的“新建邮件交换器”菜单项。出现图 5-15 所示的界面。



图 5-15　新建邮件交换器

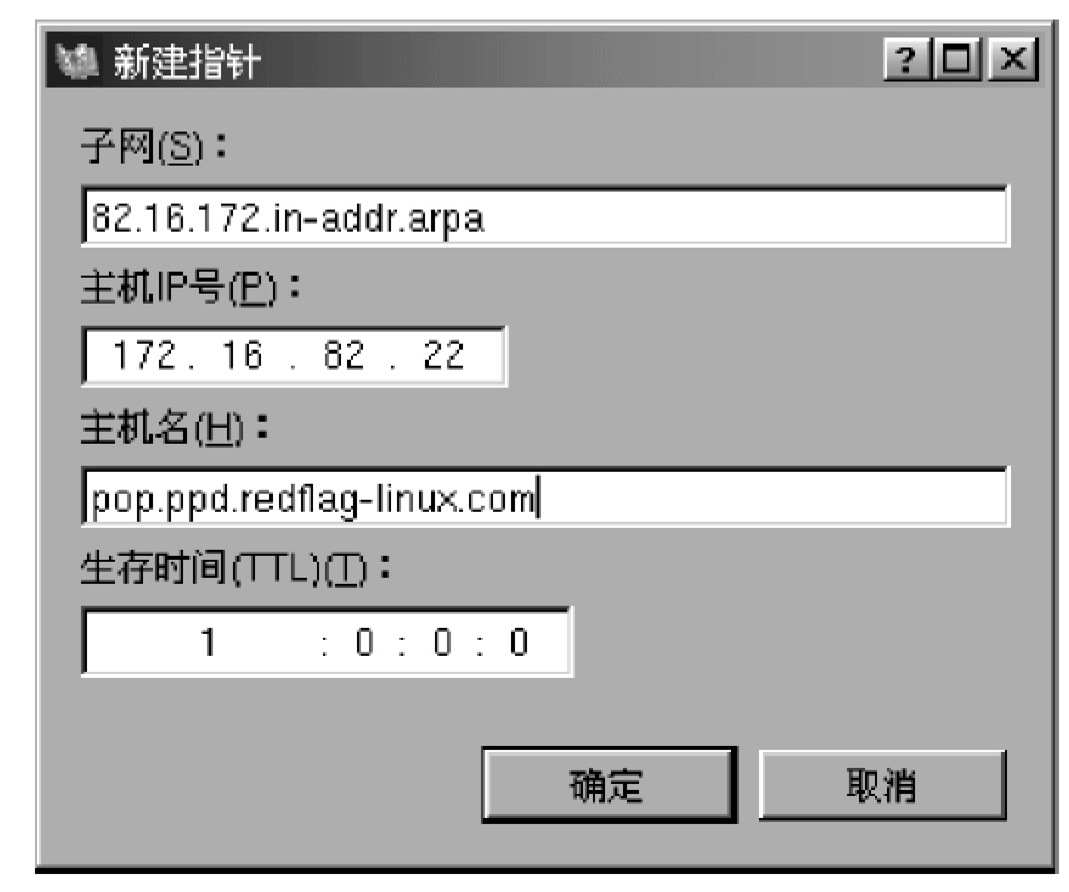


图 5-16　新建指针

在“主机或域”文本框中，输入使用此记录发送邮件的域的名称。在“邮件服务器”文本框中，输入邮件交换器或邮件服务器主机（发送指定域名的邮件）的 DNS 主机计算机名。如有需要，可以调整此区域的“邮件服务器优先级”。单击“确定”按钮，完成新增邮件交换的动作，新增的邮件交换器记录将显示在主窗口右侧的列表中。

4. 向反向区域添加指针（PTR）资源记录

在配置工具主窗口左侧的控制台树中，选择适当的反向搜索区域。单击菜单中的“操作”→“新建指针”，也可以右击选择快捷菜单的“新建指针”菜单项，弹出如图 5-16 所示的界面。

在“主机 IP 号”文本框中，输入主机 IP 地址的 8 位字节数。在“主机名”文本框中，输入 DNS 主机的完全合格域名，该计算机使用此指针记录提供反向搜索（地址—名称解析）。单击“确定”按钮，建立新增的指针，新增的指针记录将显示在主窗口右侧的列表中。

5. 修改区域中的现有资源记录

在配置工具主窗口左侧的控制台树中，单击相应的区域。窗口右侧会显示该区域的详细信息列表信息，选择要修改的资源记录项。

选择菜单中的“操作”→“属性”，也可以右击选择快捷菜单中的“属性”菜单项。在相应的属性对话框，可以根据需要查看或编辑任何可以修改的属性。

6. 从区域中删除资源记录

在配置工具主窗口左侧的控制台树中，单击相应的区域。窗口右侧会显示该区域的详细信息列表信息，选择要删除的资源记录项。

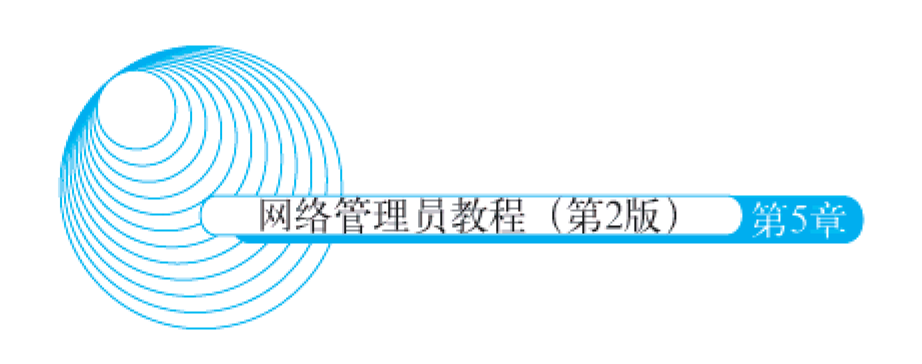
选择菜单中的“操作”→“删除”，也可以右击选择快捷菜单中的“删除”菜单项。出现提示对话框时，请确认是否删除所选的资源记录。

7. 使用 rfdns 的编辑器

为了使用户能够全面的配置 DNS 服务器支持的全部功能，rfdns 配置工具中提供了一个配置文件编辑器。用户可以通过它直接对 DNS 配置文件进行手工修改。在菜单中选择“查看”→“编辑器”，可以切换配置文件编辑窗口的隐藏与显示。

选中某一区域或资源记录时，其所对应的配置文件内容会在配置文件编辑器中被高亮显示出来。对相应配置文件进行编辑后，单击工具栏中的“存储配置文件”按钮。

配置工具也可以检查配置文件的语法错误，检查结果会显示在消息窗口中。如果出现语法错误，请根据提示进行修改。在开始手工修改配置文件后，请不要在存储之前使用配置工具提供的其他配置功能，否则所做的修改将会被覆盖。配置文件修改并存储后，必须重新启动 DNS



服务器才能使修改生效。

5.2 Apache Web 服务器配置

Apache Server 是目前使用最为广泛的 Web 服务器之一，它可以在 UNIX 和 Windows 平台上运行，对于 Linux 和 FreeBSD 系统，Apache Server 更是首屈一指的 Web 服务器。

Windows Server 2003 内置的 IIS6 组件也提供了 Web 服务功能，配置管理比较简单，因篇幅所限，这里不做介绍。本节只介绍 Red Flag Server 4.0 系统中的 Apache。

rfapache 是中科红旗软件公司推出的全新的 Apache Server 图形化配置工具；它根据 Apache Server 自身的特点，结合 Windows 系统管理员使用 IIS 的习惯；提供了一个友好、易用的图形化配置界面。在具体实现上，rfapache 通过一个友好的交互界面接受用户的命令，并完成 Apache 服务软件 httpd 相关配置文件的修改，这样管理员可以不必编辑复杂的配置文件，使配置任务变得直观和容易实现。

5.2.1 启动 rfapache

rfapache 配置工具需要在 KDE 环境下以 root 权限运行。非 root 用户虽然允许运行和使用配置工具，但由于没有权限修改配置文件，所以即便在配置工具中修改了选项也无法保存和生效。可以采用以下方法启动 rfapache 工具：

(1) 在系统主菜单中选择“系统”→“控制面板”，打开控制面板，在“网络服务配置”标签页中，双击“Apache 配置工具”；

(2) 在系统主菜单中选择“管理工具”→“Apache 配置工具”；

(3) 在运行命令行或 shell 提示符下直接输入 rfapache。

图 5-17 所示为 rfapache 的配置主界面。窗口左侧是 Apache Server 的控制台树，显示了服务器主机中构建的主机站点和目录的树状结构；窗口右侧从上到下依次为列表显示区、配置文件编辑器、配置文件跳转器和消息显示窗口。利用“显示”菜单，可以切换配置文件编辑器、配置文件跳转器和消息显示窗口的隐藏和显示。

在左侧的控制台树中选中某一节点时，列表显示区将出现该节点中的内容，可以按名称、类型或路径名排序。如果选中的是一个目录，则显示该目录中的所有子目录和文件。

管理员可以在配置文件编辑器中手工修改配置文件，并保存。消息显示窗口显示的是 Apache 服务器启动、重启、停止或校检配置文件等的输出信息。

5.2.2 启动和停止 Apache 服务

打开 Apache 配置工具 rfapache，在主界面窗口中：

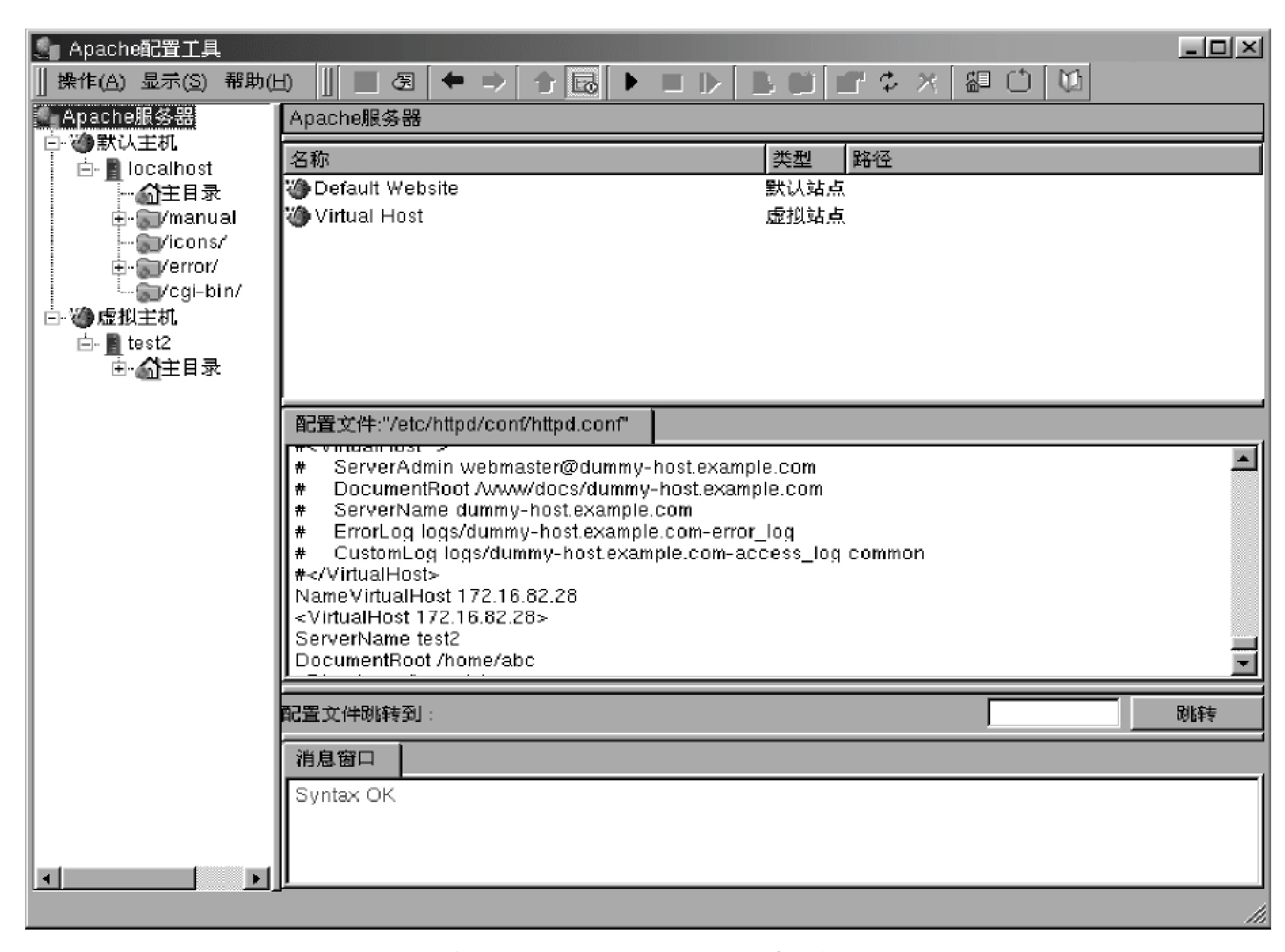


图 5-17　rfapache 配置主界面

- 单击菜单栏中的“操作”→“启动”，启动 httpd 服务；
- 单击菜单栏中的“操作”→“停止”，停止 httpd 服务；
- 单击菜单栏中的“操作”→“重启”，重新启动 httpd 服务。

如果 httpd 服务已经启动，那么菜单项“操作”→“启动”不可用；如果 httpd 服务没有启动，那么菜单项“操作”→“启动”和“操作”→“重启”不可用。

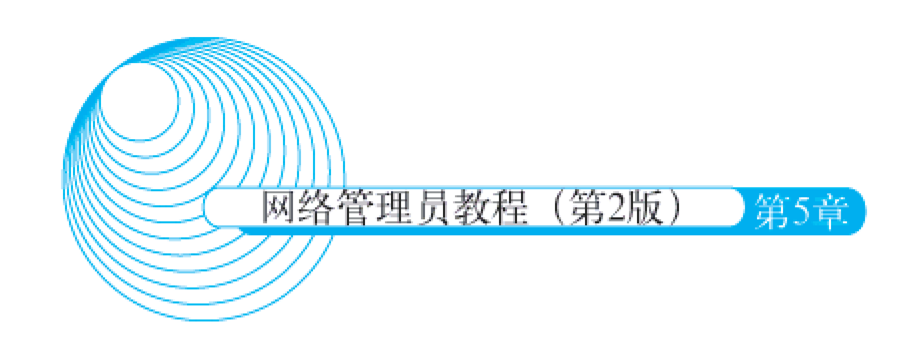
操作结果的输出信息将显示在消息窗口中。

管理员也可以在命令行终端下，通过下列命令执行大多数这些任务：

```
# /etc/init.d/httpd start
# /etc/init.d/httpd stop
# /etc/init.d/httpd restart
```

5.2.3　添加和删除虚拟主机

虚拟主机是指在一个单一的服务器上维护多个 Web 站点，并且使用主机别名来区别它们。这样用户就可以在单一的 Web 服务器上拥有多个的 Web 站点，并通过它们各自的域名对这些



站点进行访问，如 www.company1.com 和 www.company2.com，而无需用户了解任何其他路径信息。

随着因特网上的 Web 站点数目逐渐增多，在一台服务器上有效驻留多个 Web 站点的能力已经成为第一流 Web 服务器引擎的关键特性。Apache 提供了对虚拟主机的完全支持。虚拟主机一般有两种形式：“基于名字”和“基于 IP”。

1. 添加虚拟主机

Apache 配置工具中提供了一个虚拟主机的创建向导。打开 rfapache，在菜单中选择“操作”→“添加虚拟主机”，或者单击工具栏中的“添加虚拟主机”按钮，按照“虚拟主机创建向导”中的指示完成操作。

通过这个向导，管理员可以定义虚拟主机的主机名、IP 地址和端口、主目录、规划用户的访问权限等，在向导的最后，列出了新建虚拟主机的概要信息。当设置出现下列问题的时候，工具将给出错误提示，提示重新设置。

- 对于“基于名称”的虚拟主机，设置的主机名已经被其他虚拟主机使用；
- 对于“基于 IP”的虚拟主机，选择的 IP 地址（端口）已经被其他虚拟主机使用；
- 指定的主目录不存在或不是一个合法的路径。

创建虚拟主机时，需要保证所创建的虚拟服务器名能够在 DNS 中正确解析。

2. 删除虚拟主机

在 rfapache 配置工具主窗口左侧的控制台树中，选择需要删除的虚拟主机名。单击菜单中的“操作”→“删除”，或单击工具栏中的“删除”按钮，当被询问是否确认要删除该主机时，单击“确定”按钮即可。

5.2.4 添加和删除虚拟目录

虚拟目录的概念源于 Alias 和 ScriptAlias 指令，一般称“别名”。这样的指令可以将一个 URL 以非标准方式映射到一个目录文件名；也就是说可以将文档存储在服务器定义的主目录（DocumentRoot）以外的位置。例如：Alias /icons″/usr/local/apache/icons″，意思就是将文档放在 /usr/local/apache/icons 下，并通过/icons 别名来访问。

通过别名访问时，要在别名后加一个斜线后缀“/”，以上面的例子来说，访问时请求 http://localhost/icons 将会失败，因为服务器只能对 http://localhost/icons/ 作出响应，所以访问时正确输入的 URL 应该是后一种。

1. 创建虚拟目录

在 rfapache 配置工具主窗口左侧的控制台树中，选择虚拟目录要添加的位置（默认主机或

者是虚拟主机）。单击菜单中的“操作”→“添加虚拟目录”，或者单击工具栏中的“添加虚拟目录”按钮，在弹出的“虚拟目录创建向导”中，根据提示创建一个新的虚拟目录。

利用这个向导，管理员可以定义虚拟目录的别名、目录的路径、规划用户的访问权限等；在向导的最后，列出了新建虚拟目录的概要信息。当设置出现下列问题的时候，工具将给出错误提示，提示重新设置。

- 设置的别名已经存在；
- 设置的目录路径不合法；
- 设置的目录已经被其他别名映射。

2．删除虚拟目录

在 rfapache 配置工具主窗口左侧的树状结构中，选择需要删除的虚拟目录。单击菜单中的“操作”→“删除”，或单击工具栏中的“删除”按钮，当被询问是否确认要删除该虚拟目录时，单击“确定”按钮即可删除。

5.2.5 设置属性

可以在配置工具 rfapache 中设置“默认主机”、“虚拟主机”和“虚拟目录”的属性。

在 rfapache 配置工具主窗口左侧的控制台树中，选择需要查看或设置属性的主机或目录。单击菜单中的“操作”→“设置属性”，或者单击工具栏中的“设置属性”按钮，也可以单击鼠标右键，从快捷菜单中选择“设置属性”，在弹出的属性设置窗口中查看或修改相应的属性。属性设置窗口中包括了多个配置标签页，具有相当多的选项可供设置，下面分别加以说明。

1．站点属性

站点属性标签如图 5-18 所示。使用此标签页设置站点的标识参数和日志信息等，只有默认主机和虚拟主机有此属性设置页。

1）站点设置

（1）站点名称（配置项：ServerName）：设置 Web 服务器的主机名。可以任意指定站点名称，此名称将出现在 rfapache 主窗口的控制台树视图中。

注意：设定的服务器主机名必须在 /etc/hosts 文件中或在 DNS 中能够解析。

（2）管理员 Email（配置项：ServerAdmin）：设定 Web 管理员的 E-mail 地址，用于在 Web 连接和服务出错时，用该地址向管理员发送出错消息。

（3）IP 地址：用来指定主机的 IP 地址，单击“高级”按钮，可以配置 IP 地址。

（4）TCP 端口：指的是服务器监听客户请求的端口，默认为 80，也可以分配其他端口号。如果这样做，访问 Apache 服务器时就必须在 URL 后面跟上端口号才能访问到页面，即 http://



图 5-18 “站点属性”标签页

apacheserver:port。

2）错误日志

用来告诉服务器错误日志文件的路径和名称。如果不需要强制指定错误日志文件的路径和名称;选择“默认值”选项。其中,日志位置的默认值为 logs/error_log,日志类型的默认值为 error。

（1）日志位置(配置项：ErrorLog)：用来指定错误日志文件的位置。如果该位置不是以斜线(/)开头,就是相对于配置的服务器根目录而言的。这里的位置可以是：

① 完整路径,如/var/logs/apache/error_log;

② 相对路径,如 logs/new_log(以 ServerRoot 目录为相对路径);

③ 实用程序 syslogd。

打开一个指向程序或者脚本的系统管道,所指向的程序或脚本是负责将错误信息写入日志的,如：ErrorLog | /usr/local/apache/logfilter. pl。很容易编写这样的一个 Perl 脚本,以便当特定消息写入日志时立即通知系统管理员。

（2）日志级别(配置项：LogLevel)：用于指定 Apache 在错误日志记录中使用 8 种细节级别的哪一种。表 5-2 列出了这些级别,它们分别和 Linux 系统日志中的相同错误级别对应。

表 5-2 日志级别

级别	说明	级别	说明
emerg	将导致系统无法使用的紧急情况	warn	警告状态
alert	要求立即作出响应操作	notice	建议状态，并不表示有异常活动
crit	关键状态	info	普通信息
error	错误状态	debug	只在调试模式运行时显示的信息

需要指出的是，如果将 LogLevel 设置为 warn，那么 Apache 也会把 emerg、alert 、crit 和 error 级别中定义的所有错误信息写入日志。

3）自定义日志

供系统管理员记录对服务器的所有访问，与错误日志记录不同的是，如果没有指定确定的访问日志位置，系统就不对访问进行记录。对错误日志而言，即使不用 ErrorLog 指令指定，错误日志也会记录到一个默认位置。

（1）日志位置（配置项：CustomLog）：指定日志文件的路径和文件名，还可以选择是否在日志文件中使用一个定义好的日志格式。

（2）日志格式、详细格式（配置项：LogFormat）：本配置项包括两部分，一个是格式字符串（详细格式），另一个是用于指代确定的格式的代用名（日志格式）。

2. 主目录

主目录标签如图 5-19 所示，使用此标签页修改主目录的路径，设置主目录的执行属性。

1）目录路径（配置项：DocumentRoot）

用来定义 Apache 提供文件的顶级目录，这个目录应该包含 Apache 收到 URL 请求时提供的文件。

2）目录的执行设置（配置项：Options）

用来控制对于该目录，哪些服务器功能是有效的，界面选项与配置项的对应见表 5-3。默认的设置是 All，它准许除 Multiviews 以外的所有功能。如果选择了 None，则禁用所有的功能。

表 5-3 目录执行配置项

配置项	界面选项
All	准许所有功能（Multiviews 除外）
None	禁用所有功能
ExecCGI	准许执行 CGI
FollowSymlinks	跟随符号链接

续表

配置项	界面选项
Indexes	没有 Index 文件时显示目录所有文件
Multiviews	允许内容协商的 Multiviews
SymLindsIfOwnerMatch	跟随同一个用户 ID 拥有的符号链接
Includes	允许服务器方包含(SSI)
IncludesNOEXEC	允许 SSI,但禁用 SSI 中的 ＃exec 和 ＃Includes

3）目录别名(配置项：Alias)

只有虚拟目录中才有该配置项,用来指定虚拟目录的别名。

3. 访问许可

访问许可标签如图 5-20 所示,访问许可的主要功能是用来根据 IP 地址或域名等来授权或者禁止对资源的访问。



图 5-19 “主目录”标签页

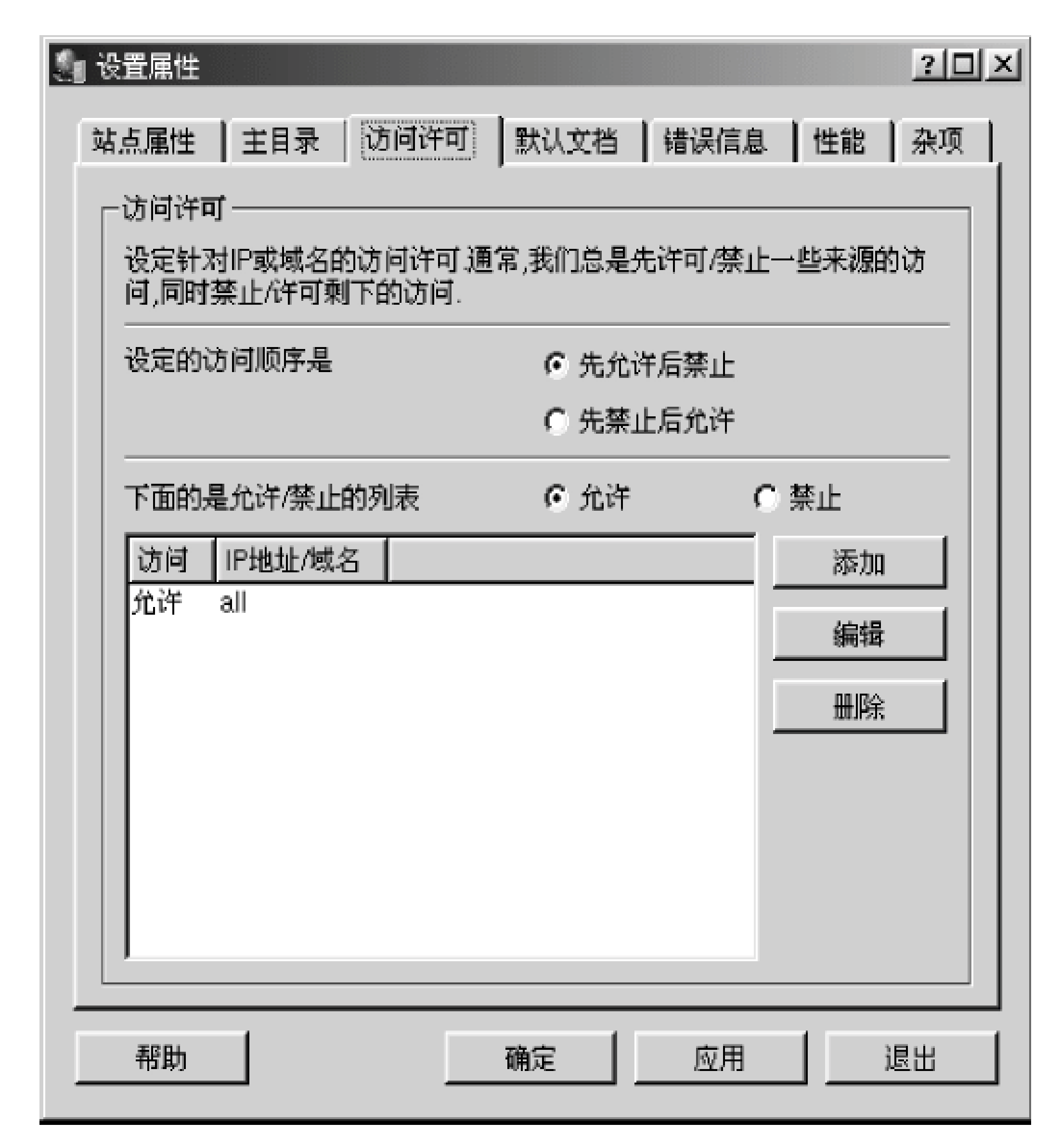


图 5-20 “访问许可”标签页

1）访问顺序(配置项：Order)

用来确定 allow 和 deny 指令应用的顺序,基本上有如下两种形式。

(1）先禁止后允许：所有 deny 指令都在 allow 指令之前应用。这种访问顺序一般用来禁止大多数主机对一个目录的访问,只允许选定的一部分主机进行访问。这种情况很像严格限制的防火

墙(允许情况最少)规则：首先是拒绝所有客户的普通访问,然后只允许数量有限的用户访问。

(2) 先允许后禁止：所有 allow 指令都在 den 指令之前应用。这种访问顺序一般用于允许大多数客户的访问,而只是指定的一些主机被禁止。

2) 允许访问列表(配置项：Allowfrom)

通过 IP 地址或域名指定允许访问相关目录资源的主机。

3) 禁止访问列表(配置项：Denyfrom)

通过 IP 地址或域名指定禁止访问相关目录资源的主机。

4. 默认文档

默认文档标签如图 5-21 所示,使用此标签页定义站点的默认页面。默认文档的配置项是 DirectoryIndex。

在这里设置请求指定目录时该目录的索引文件。如果 Apache 配置中不包括任何 DirectoryIndex 指令,当 URL 请求解析为一个目录时,它将查找并试图提供一个名字为 index.html 的文件。虽然这是一种默认方式,但标准 Apache 配置还是会在 httpd.conf 文件中创建这样的一行：DirectoryIndex index.html。

用户可以定义多个这样的索引文件,例如：DirectoryIndex、index.html、index.php 等。若要添加新的默认文档,单击“添加”按钮。

注意：*多个索引文件的前后顺序决定了服务器返回的文档的顺序。可以在配置窗口中通过“上移”和“下移”按钮调整这些索引文件的顺序。*

5. 错误信息

错误信息标签如图 5-22 所示,错误信息的配置项是 ErrorDocument。如果 Apache 在处理用户请求时遇到错误,它将按照配置显示一个标准错误页并给出 HTTP 响应代码。使用 ErrorDocumnet 指令并针对标准 HTTP 错误来定制成用户的错误响应,以便让用户更容易理解。

ErrorDocument 可以用两种方式来配置 Apache 响应特定的 HTTP 错误代码。第一种方式是直接显示错误文本,例如 ErrorDocument 403 “You are not authorized to view this info”;另一种是发布重定向,即告诉客户去哪里请求文档,例如：ErrorDocument 403 “/var/www/error/noindex.html”。

针对虚拟主机设置的错误信息会继承默认主机中的值,同样,虚拟目录的默认文档也会继承虚拟主机(或默认主机)中的值。

如果要添加新的自定义错误消息,单击“添加”按钮;如果要更改某一错误消息的属性,单击“编辑”按钮;如果要删除某一自定义错误消息,单击“删除”按钮。



图 5-21 “默认文档”标签页

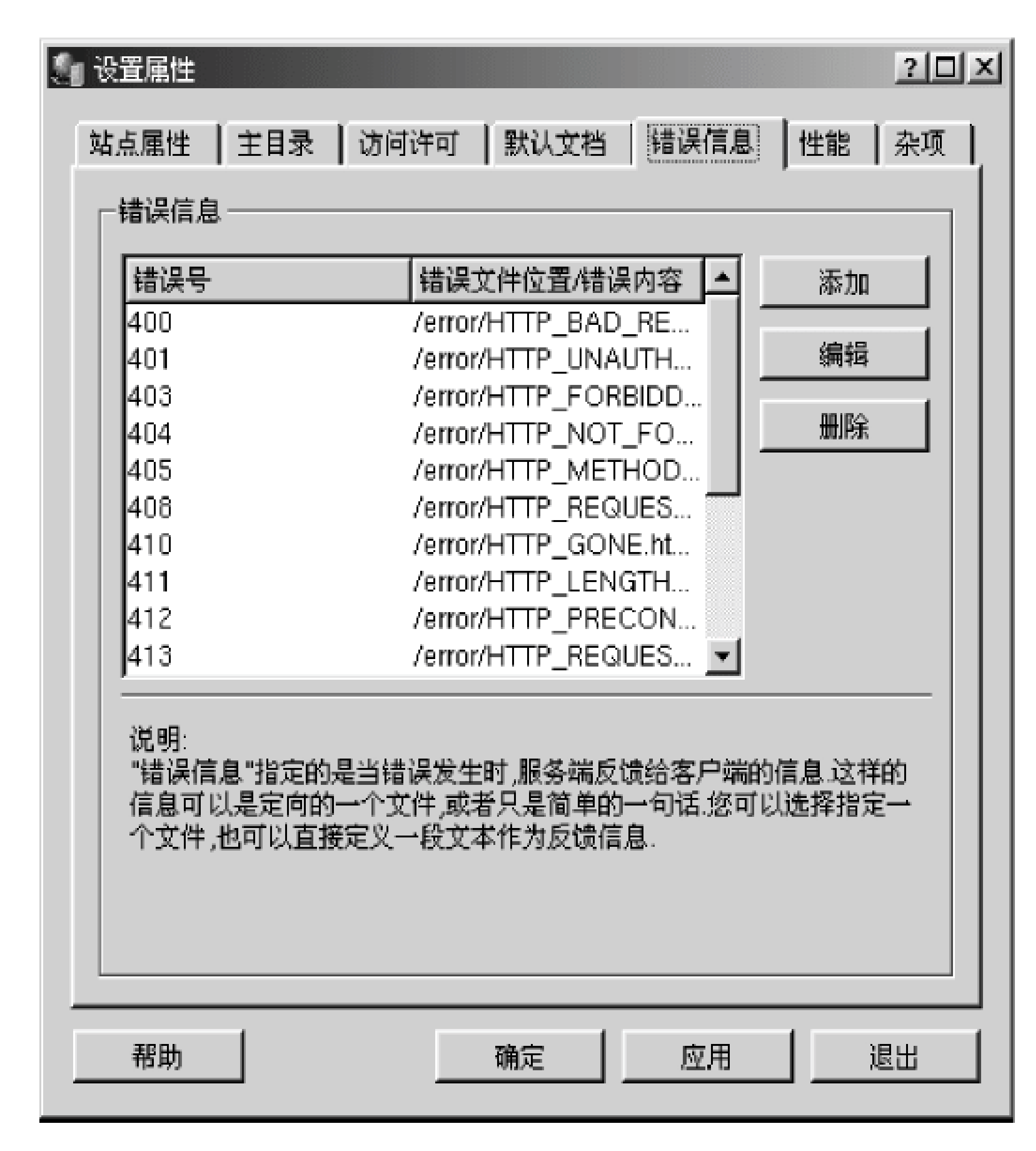


图 5-22 “错误信息”标签页

6．性能

性能标签如图 5-23 所示，用来设置一些和 Apache 运行性能有关的配置项。只有“默认主机”包含此属性配置页。

1）保持连接（配置项：KeepAlive）

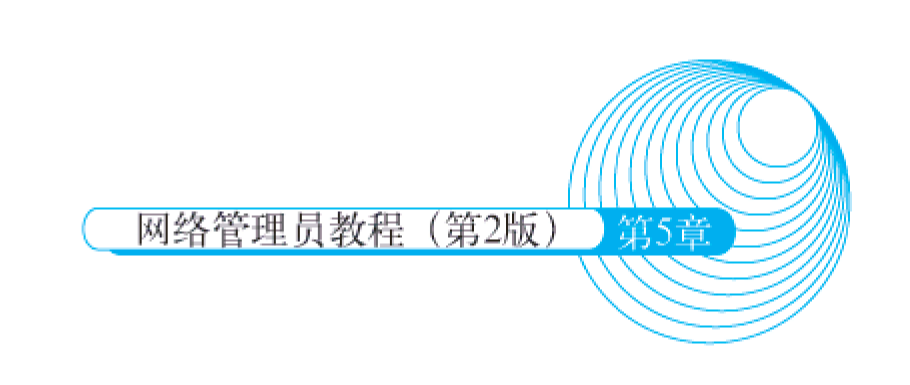
用来打开或者关闭 HTTP/1.1 持久性连接（on 或者 off），默认值为 on，意味着 Apache 允许支持持久性连接的浏览器使用此功能。符合 HTTP/1.1 规定的浏览器会使用持久性连接，通过一条 TCP 连接向 Web 服务器提交多个请求。打开这个功能通常能够获得比传统无连接高得多的速度——因为在传统无连接 HTTP 中，客户需要为每个请求都建立一条对服务器的新连接。

2）保持连接时间（配置项：KeepAliveTimeout）

用来指定 Apache 在接收一个带有 HTTP Keep-Alive 头的客户请求，要求建立持久性连接之后，等待其后续请求的时间。默认值为 15s，如果在这段时间里没有收到后续请求，Apache 在完成对当前客户请求的处理之后会关闭连接。

3）最大请求保持数（配置项：MaxKeepAliveRequests）

用来限制每条持久性连接允许的请求数量。默认值为 100，这个值对于所有网站都应该足以满足需要。如果这个值设为 0，那么对于一条连接将允许数量不限的请求。这是应该避免的，因为如果这样 Apache 服务器就会面临被恶意用户进行服务封锁攻击的危险。



4）连接超时（配置项：TimeOut）

用来设置一个超时长度，当等待来自客户的响应达到这个超时限制的时候就关闭这个连接。默认的时间长度是300s，也就是5min。

5）初始化最大进程数（配置项：StartServers）

用来指定当Apache启动时生成的空闲服务器进程的数目。默认值为5，通常很少有必要修改它，除非是对于处理负担很重的服务器，才有可能需要增大这个值，以保证进程池中有足够的Apache进程来处理数量众多的客户连接。

6）最小空闲进程数（配置项：MinSpareServers）

用来指定进程池中的最低空闲服务器数量（空闲服务器等待着输入连接）。Apache的主进程保证：总是至少有这么多的空闲服务器进程在等待处理客户请求。系统默认值是5，一般不需要调整。适当的增大这个值，让更多的服务器进程处于等待状态，这样当新进程产生时就不会感觉有太多的延迟。在处理负荷很小的服务器上应该适当减小这个值，可以避免系统内存的无谓浪费。

7）最大空闲进程数（配置项：MaxSpareServers）

用来指定进程池中的最大空闲进程数。如果空闲的进程数超过这个值，Apache主进程就会结束过多的服务器进程，直到空闲进程数少于此数目。默认值为10，同样在通常情况下不需要改动，只在处理负担很重或者很轻的系统上才进行更改。

8）单进程最大请求数（配置项：MaxRequestsPerChild）

用来定义每个子进程处理服务请求的次数。默认值为30，这个值对于具备高稳定性特点的Linux系统来讲是过于保守的设置，可以设置为1000甚至更高，设置为0则支持每个副本进行无限次的服务处理。

使用子进程的方式提供服务的Web服务，常用的方式是一个子进程为一次连接服务，这样造成的问题就是每次连接都需要生成、退出子进程的系统操作，这些额外的处理过程占据了计算机的大量处理能力。因此最好的方式是一个子进程可以为多次连接请求服务，这样就不需要这些生成、退出进程的系统消耗。Apache就采用了这样的方式，一次连接结束后，子进程并不退出，而是停留在系统中等待下一次服务请求，这样就极大的提高了性能。但由于在处理过程中子进程要不断的申请和释放内存，次数多了就会造成一些内存垃圾，就会影响系统的稳定性，并且影响系统资源的有效利用。因此在一个副本处理过一定次数的请求之后，就可以让这个子进程副本退出，再从原始的httpd进程中重新复制一个干净的副本，这样可以提高系统的稳定性。

9）最大连接数（配置项：MaxClients）

用来设置可以同时运行的httpd监听进程的数量限制。一般没有必要更改，默认值是256，无法超越这个值，这样的限制是一个安全措施，可以保证服务器免于在负担太重的时候崩溃。如果服务器的负担太重，256个进程已经显得不够，那么建议在网络中增加一台物理服务器。这个参数限制了MinSpareServers和MaxSpareServers的设置，它们不应该大于这个参数的设置。

7. 杂项

杂项标签如图 5-24 所示，用来设置一些其他常用且很重要的配置项。



图 5-23 “性能”标签页



图 5-24 “杂项”标签页

1）服务器根目录（配置项：ServerRoot）

用来指定服务器所在的目录，通常与 Apache 安装过程中的-prefix 选项设置的路径一致。配置文件中的很多相对路径（例如：logs/error_log）都是以这个目录为相对位置的。

2）服务 PID 文件（配置项：PidFile）

用来定义包含运行 Apache 服务器进程 ID（process 或 PID）文本文件的路径和文件名。但是很少有必要去改变 Apache 的默认 PID 文件，这个默认文件一般作为 httpd. pid 存储在 Apache ServerRoot 下的 logs 目录中。

3）服务 LOCK 文件（配置项：LockFile）

用来指定 httpd 守护进程的加锁文件。同样很少有必要去改变 Apache 的默认文件，这个文件一般作为 accept. lock 存储在 Apache 的 ServerRoot 下的 logs 目录中。

4）用户名（配置项：User）

用来定义拥有“处理用户请求创建”的子进程的 Linux 用户。这个指令只有在 Apache 服务器作为 root 用户启动时才有效。如果服务器作为任何其他用户启动，这个指令都不能修改子进程的所有者。

5）组名（配置项：Group）

与 User 指令一样，这个指令用来修改“处理工作且请求创建”的子进程的所有权。区别是，

这个指令不是修改这些进程的用户所有权而是修改工作组所有权。同 User 一样，Apache 服务器必须作为 root 启动时才能使用工作组指令，否则服务器不能修改任何由它生成的子进程组的所有权。

5.3 FTP 服务器配置

FTP 是 File Transport Protocol 文件传输协议的缩写，FTP 服务器是采用 FTP 协议的服务器，能够在网络上提供文件的上传与下载等传输服务。

在 Red Flag Server 4.0 系统中，可以利用 ProFTPD 构筑安全高效的 FTP 站点。ProFTPD 的设计目标是实现一个安全且易于设定的 FTP 服务器。特别是对于熟悉 Apache 配置的用户而言，对 ProFTPD 配置起来能够得心应手。它的配置和 Apache 十分相似，也是使用了一个 KDE 环境下的、图形化的 ProFTPD 配置工具 rfftp。这里不再介绍，本节主要以 Windows Server 2003 中 IIS6 里内置 FTP 模块为例，讲解配置 FTP 服务器的过程。

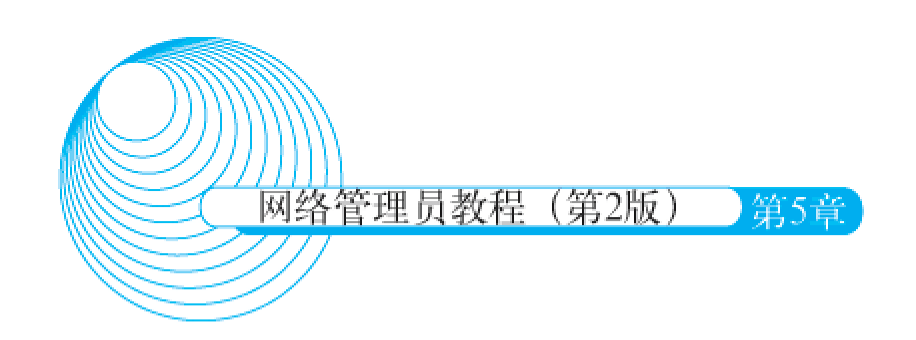
5.3.1 FTP 服务器的安装

Windows Server 2003 中 IIS 里内置 FTP 服务模块，安装较为简单。由于 FTP 不是默认的安装组件，系统不会自动安装，因此必须采用 Windows 组件方式来安装 FTP 服务。具体操作步骤如下：

（1）打开“控制面板”，双击“添加或删除程序”，单击对话框左下角的“添加/删除 Windows 组件”，如图 5-25 所示。



图 5-25 “添加或删除程序”对话框



（2）在“Windows 组件向导”窗口的“Windows 组件”列表框中选中“应用程序服务器”，如图 5-26 所示。

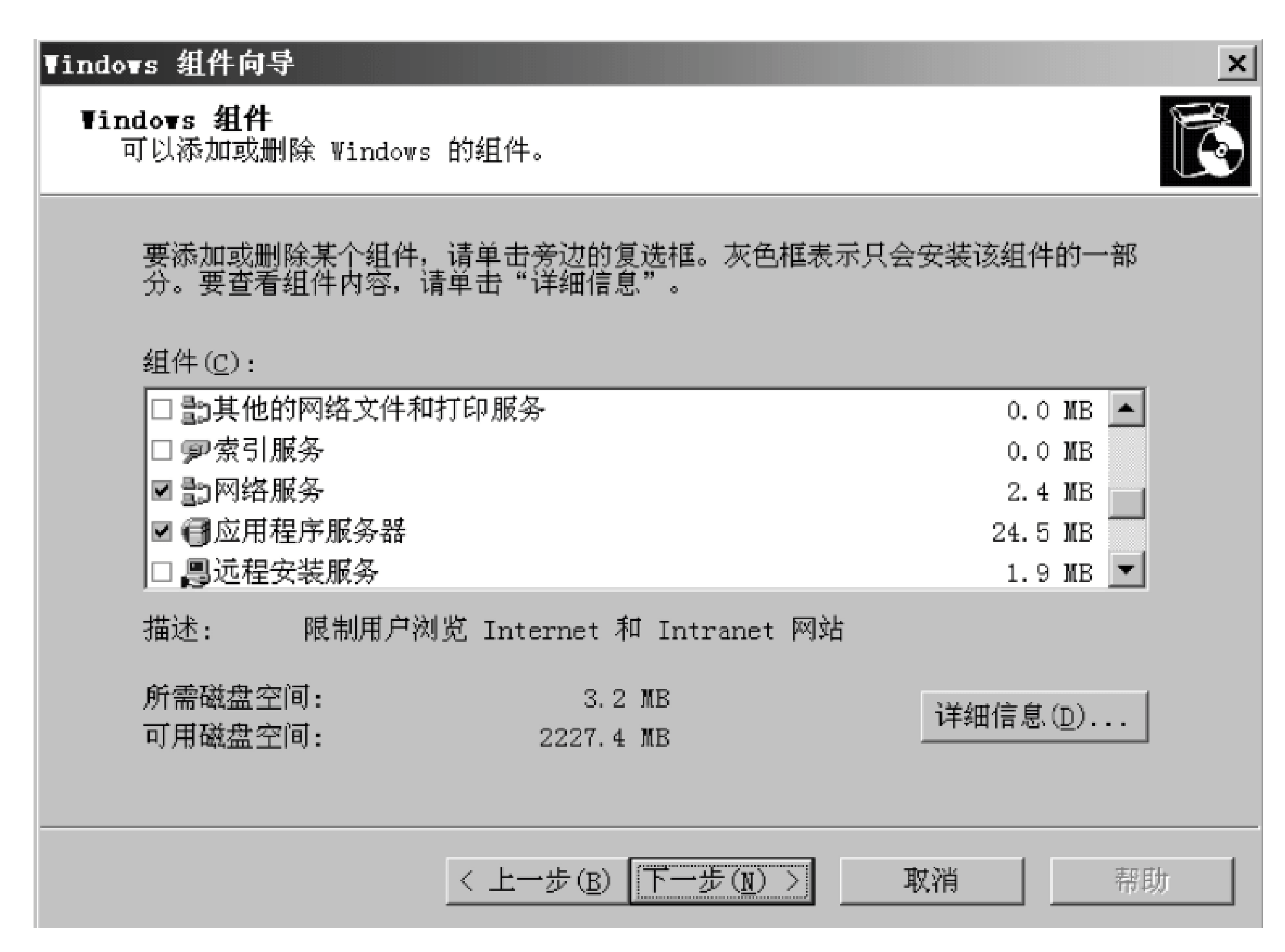


图 5-26 “Windows 组件向导”对话框

（3）单击“详细信息”按钮，弹出“应用程序服务器”窗口，选中“Internet 信息服务（IIS）”复选框，如图 5-27 所示。

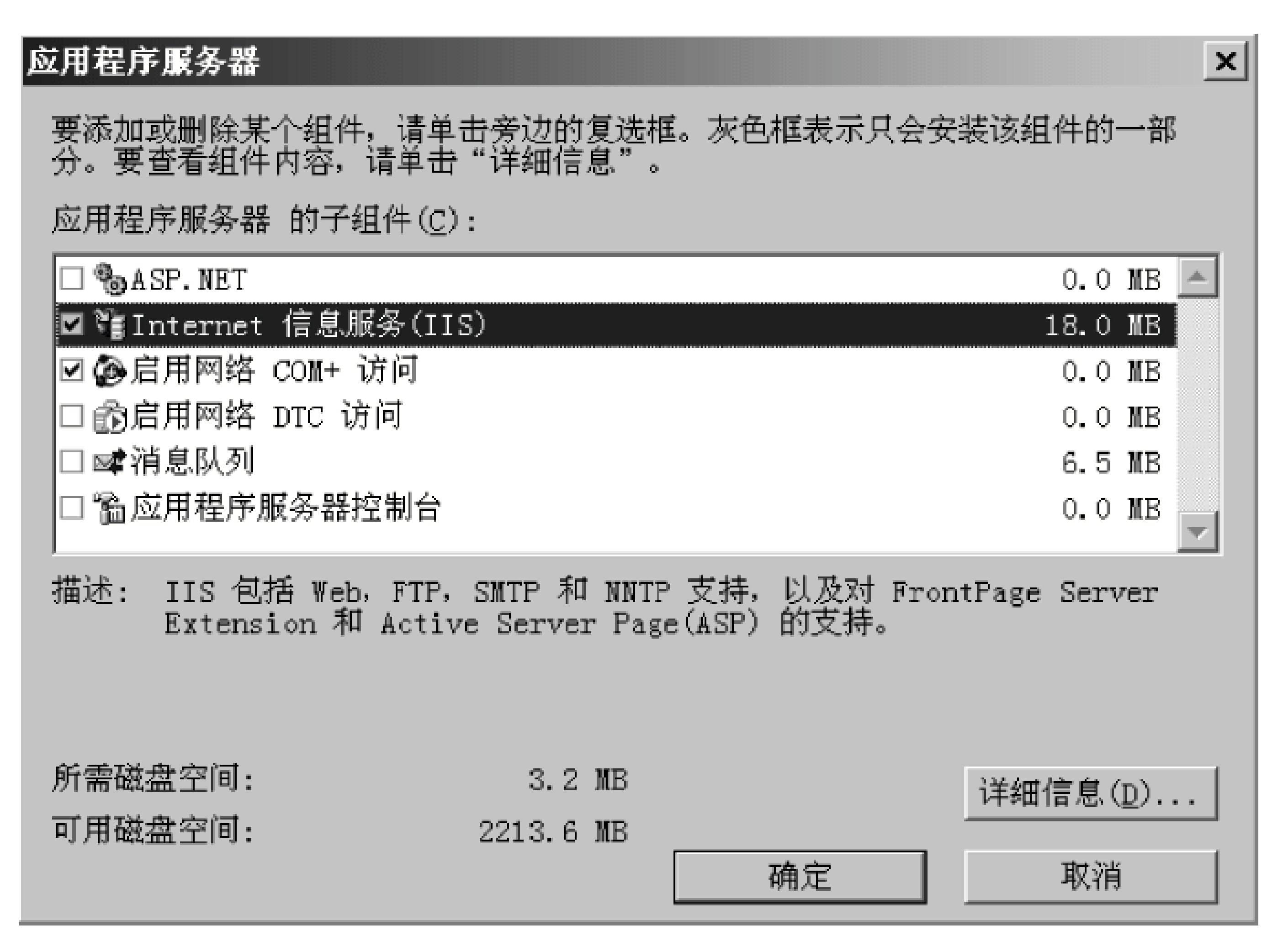


图 5-27 “应用程序服务器”对话框

(4) 系统显示"Internet 信息服务(IIS)"对话框，选中"文件传输协议(FTP)服务"复选框，如图5-28 所示，单击"确定"按钮，根据提示信息插入光盘，系统自动完成 FTP 服务的安装。

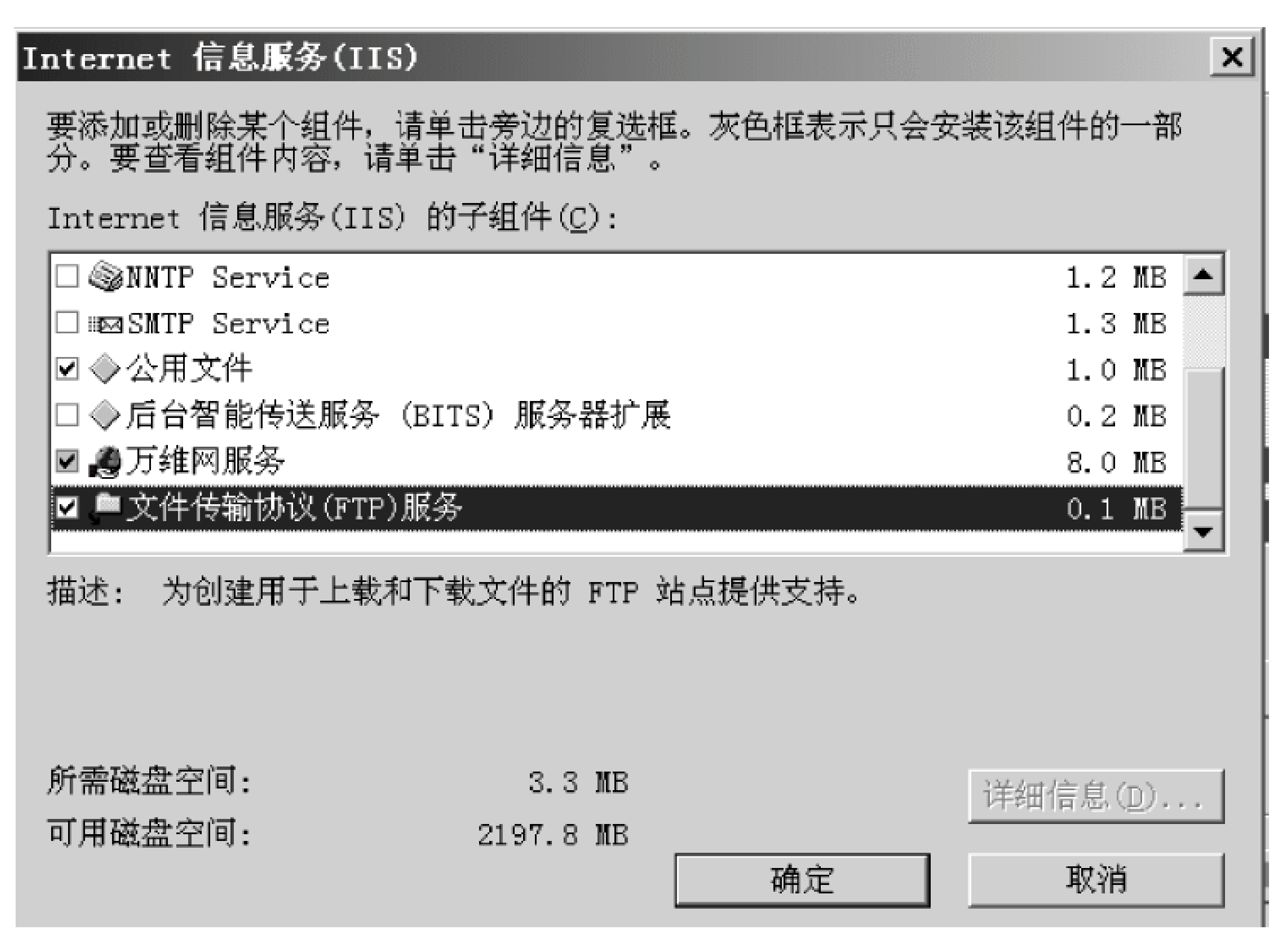


图 5-28 IIS 对话框

5.3.2 FTP 服务器的配置

已安装好的 FTP 服务器的"默认 FTP 站点"所在主目录为 C:\Inetpub\Ftproot(若系统安装在 D 盘，则为 D:\Inetpub\Ftproot)，IP 地址为"全部未分配"，允许来自任何 IP 地址的用户以匿名的方式访问。只需要将共享文件复制到 C:\Inetpub\Ftproot 目录下，FTP 客户端用户就可以匿名登录进行文件下载，但由于默认情况下主目录为只读方式，所以客户端只能下载不能上传。为了更好地管理 FTP 服务器，需要对它进行适当的配置。

1. 修改 IP 地址和端口

(1) 依次单击"开始"→"管理工具"→"Internet 信息服务(IIS)管理器"，打开 IIS 控制台，显示 IIS 信息，包括 FTP 站点、应用程序池、网站以及 Web 服务扩展等，如图 5-29 所示。

(2) 展开窗口左边的"FTP 站点"控制树，选中"默认的 FTP 站点"，单击工具条上的按钮可以实现对 FTP 站点的启动、暂停、停止等操作。

(3) 右击选择属性子菜单，系统显示 FTP 站点属性信息，如图 5-30 所示。其中"FTP 站点"选项卡包括 FTP 站点的标识、FTP 站点连接和日志记录信息，其中 IP 地址和端口号在 FTP 站

点的标识中设置。

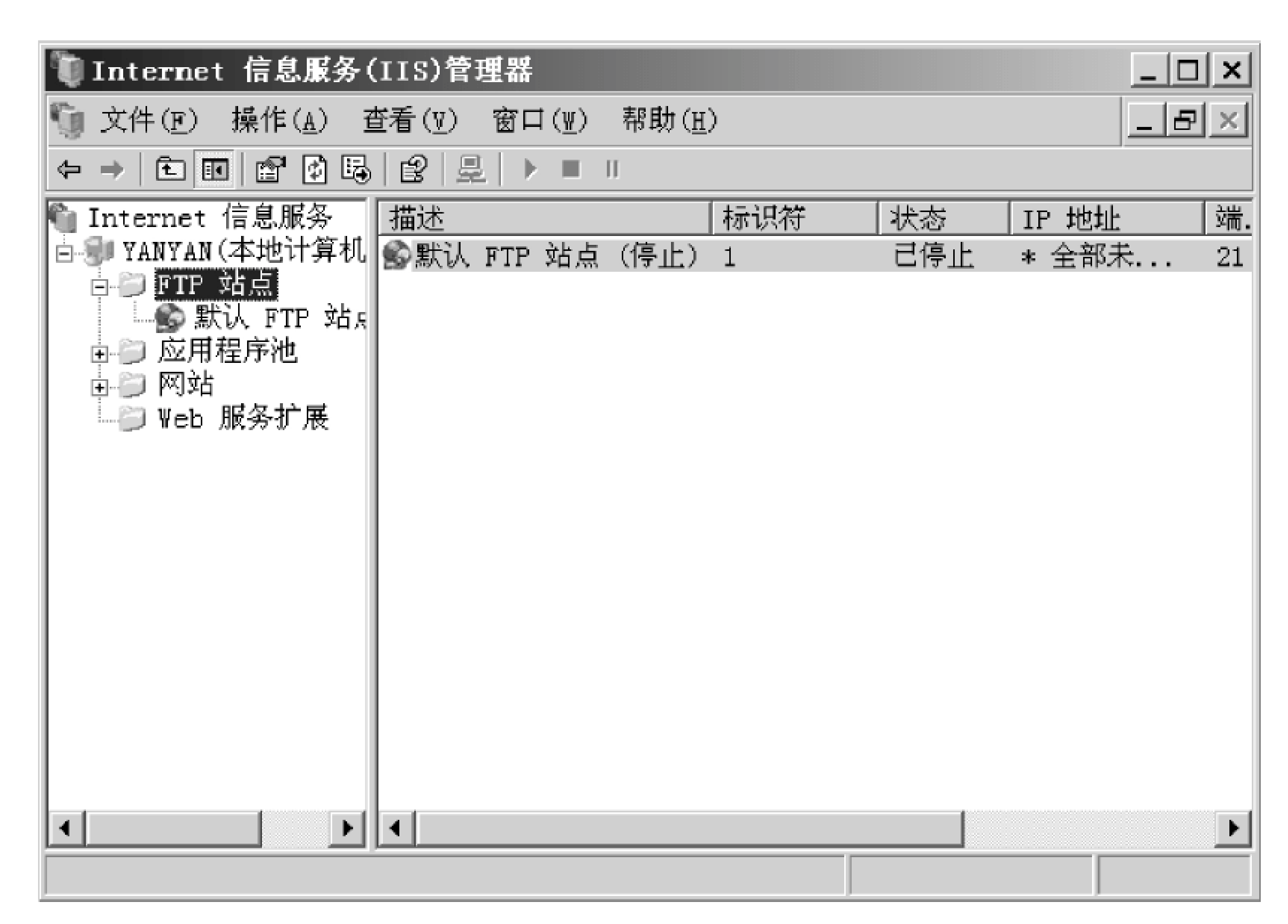


图 5-29 IIS 管理器

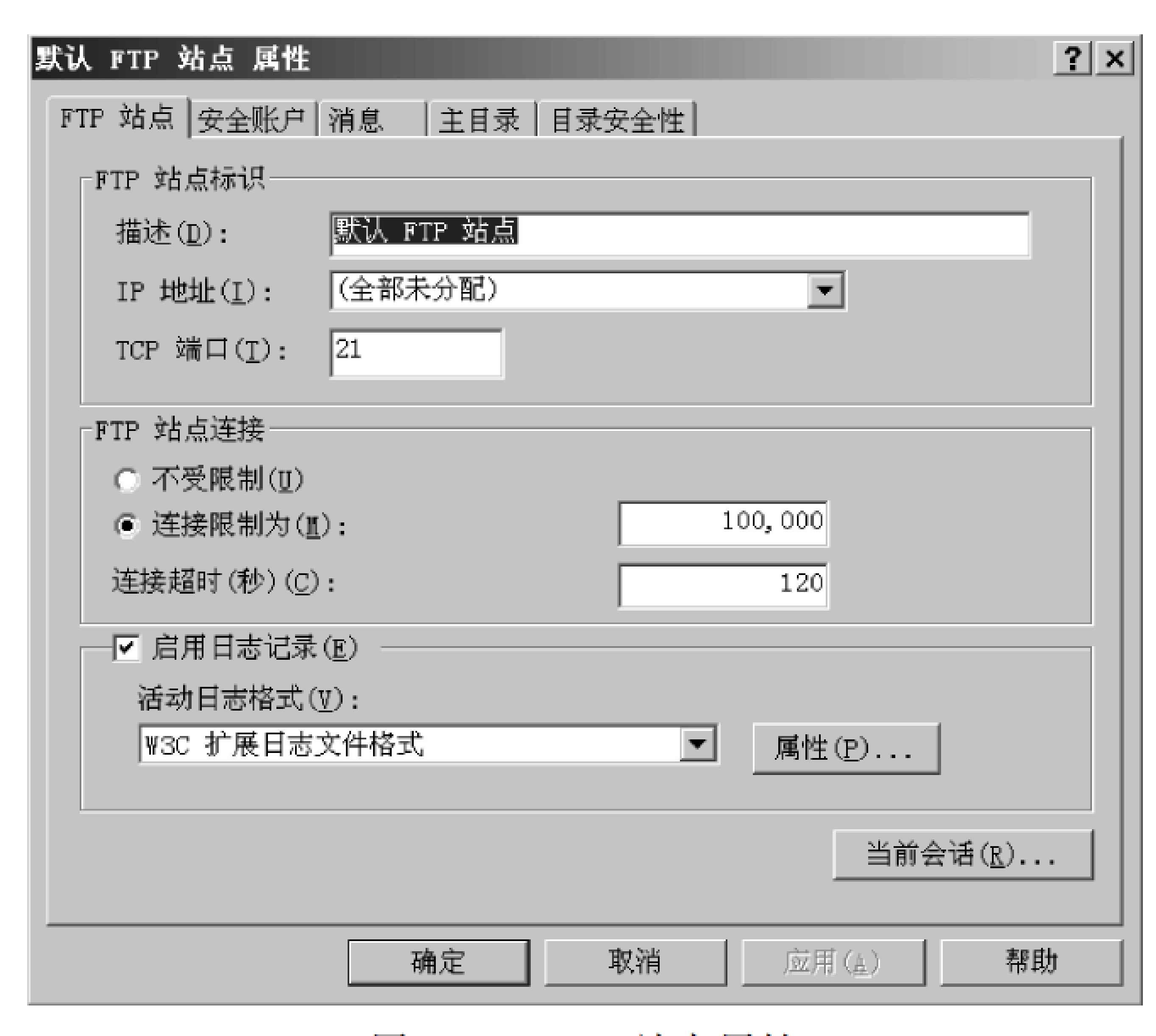


图 5-30 FTP 站点属性

“描述”作为 FTP 服务器的名称显示在“Internet 信息服务”窗口的目录中，如果在一台计算机中安装了多个 FTP 服务器，管理员可根据“标识”对各台 FTP 服务器加以区分。

“IP 地址”列表中设置该 FTP 站点的 IP 地址。Windows Server 2003 操作系统中允许安装有多块网卡，而且每块网卡也可以绑定多个 IP 地址，通过设置“IP 地址”文本框中的信息，FTP 客户端利用设置的这个 IP 地址来访问该 FTP 服务器。通过下拉列表从一个或多个地址中选择一个作为“IP 地址”。

“TCP 端口”是指用户与 FTP 服务器进行连接并访问的端口号，默认的端口号为 21。服务器也可设置一个任意的 TCP 端口号，若更改了 TCP 端口号，客户端在访问时需要在 URL 之后加上这个端口号，因此必须让客户端事先知道，否则就无法进行 TCP 连接。

比如可以设置标识为 MP3，IP 地址为 192.168.0.61，端口号为 21，如图 5-31 所示。

图 5-31　配置 FTP 站点属性

2. 限制连接数量

在“FTP 站点”选项卡的“FTP 站点连接”中有 3 个选项。

(1) 不受限制：该选项允许同时发生的连接数将不受任何限制。

(2) 连接限制为：该选项限制允许同时发生的连接数为某一特定值，这一特定值由用户在文本框中输入。

(3) 连接超时：当连接超时为某一值时服务器断开。

由于服务器配置、性能等的差别，有些服务器不能满足大访问量的需要，往往造成超时甚至死机，因此需要设置连接限制。同时，为了确保 FTP 协议在连接失败时关闭连接，因此需要设置连接超时。

3. 设置主目录

主目录信息在属性信息的“主目录”选项卡中设置。所谓主目录是指映射为 FTP 根目录的文件夹，FTP 站点中的所有文件将保存在该目录中。系统默认的 FTP 主目录为 C:\Inetpub\Ftproot（其中，C 为操作系统安装的逻辑盘符，若系统安装在 D 盘，则为 D），可以根据用户的需要更改主目录和其属性。

可以把主目录修改为计算机中的其他文件夹，甚至可以是另一台计算机上的共享文件夹。同时，管理者可以修改用户对站点的访问权限，以及目录的列表风格，如图 5-32 所示。

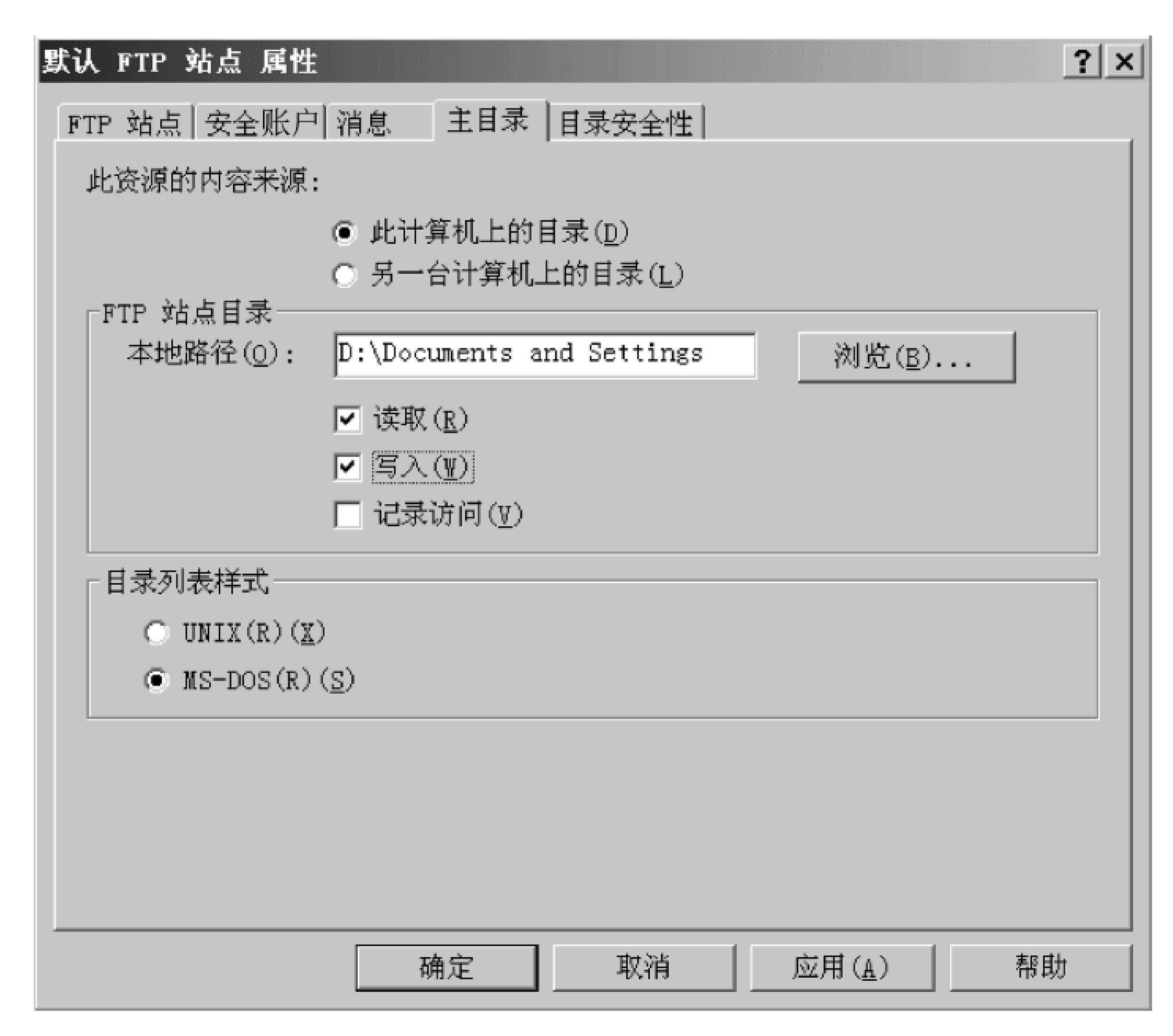


图 5-32 FTP 站点主目录属性

4. 访问安全设置

FTP 站点的安全非常重要，Windows Server 2003 中对 FTP 服务器可配置用户身份认证、限制访问 FTP 的 IP 地址，从而确保站点的安全。

(1) 禁止匿名访问。禁止匿名访问在属性信息的“安全账户”选项卡中设置。在默认情况下，FTP 站点允许用户匿名访问，如果站点安全性要求较高，取消选中“允许匿名连接”即可禁止

用户匿名访问该 FTP 站点，如图 5-33 所示。

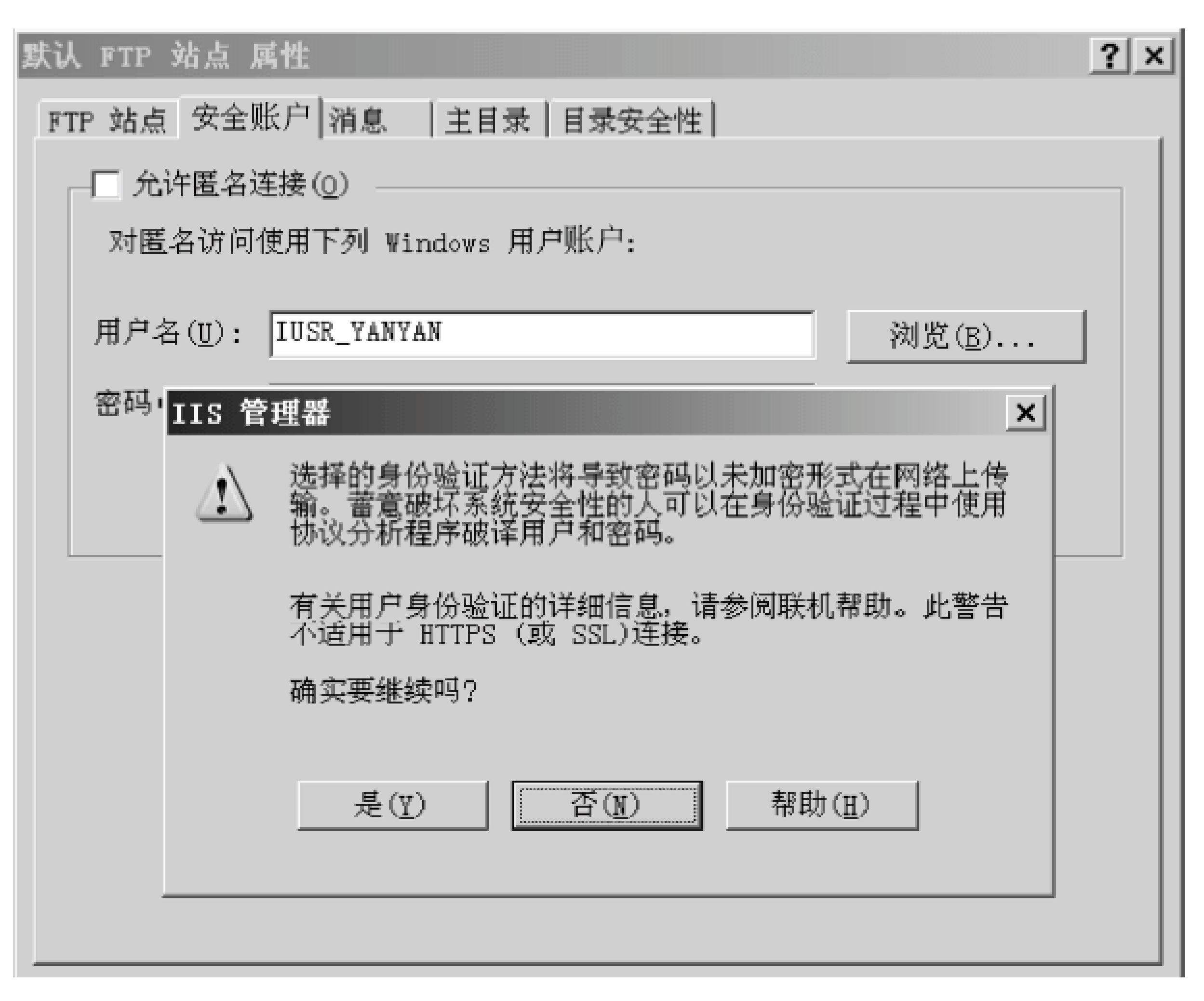


图 5-33　FTP 服务器的匿名用户设置

（2）限制 IP 地址。限制 IP 地址在属性信息的“目录安全性”选项卡中设置。通过对 IP 地址的限制可以只允许某些特定范围的计算机访问该站点，从而避免外界恶意攻击，如图 5-34 所示。



图 5-34　FTP 服务器的限制 IP 地址设置

此外，还可以对 FTP 服务器的磁盘限额和提示信息等做相应的配置。

5.4 配置电子邮件服务器

电子邮件是因特网服务的重要组成部分，随着因特网技术日新月异的发展，电子邮件以其方便、快速、廉价的特点越来越赢得人们的喜爱。电子邮件系统中有两个至关重要的服务器：SMTP(发件)服务器和POP3(收件)服务器。平时在发送邮件时，其实只是把邮件发送到发件服务器上，而服务器使用一种叫做“存储转发”的技术，把它收到的电子邮件排队，依次发送到收件服务器上面，而邮件就一直存储在收件服务器上，直到收件人收信或直接删除。安装和配置电子邮件服务器的主要工作，就是对这两个服务器(逻辑上的)进行操作。

在红旗Linux操作系统上，基于Web的电子邮件系统Red Flag Webmail Server 4.0。它是一款面向政府、机关、中小型企业、学校等中小规模用户的邮件系统。Red Flag Webmail Server 4.0系统作为大容量邮件系统，在产品性能上具有很高的稳定性、可靠性和安全性，是一个专业的电子邮件系统平台。相对比而言，Windows Server 2003新增加的邮件服务器(POP3)，配置非常简单，只需几个步骤就可以完成。但与专业的邮件服务器相比它只能算是一个具备收发邮件功能的简单服务器，尚未涉及到容量控制、邮件转发、用户信息维护等功能。对于初学者来说，它是一个不错的学习软件。下面借助Windows Server 2003系统新增加的POP3服务组件来创建一个简单的邮件服务器。

5.4.1 电子邮件服务器的安装

(1) 依次单击“开始”→“管理工具”→“管理您的服务器”，将出现服务器管理窗口，单击“添加或删除角色”连接，单击“下一步”按钮，系统显示“服务器角色”对话框，选中“邮件服务器(POP3，SMTP)”，如图5-35所示。

(2) 单击“下一步”按钮，系统弹出“配置POP3服务”窗口，其中包括身份验证方法和电子邮件域名两部分。身份验证方法包括本地Windows账户身份验证和加密密码文件两种验证方式。选择身份验证方式、输入电子邮件域名，如图5-36所示。

(3) 单击“下一步”按钮，显示“选择总结”对话框，如图5-37所示。

(4) 确认选择后，单击“下一步”按钮，按照系统提示插入光盘，如图5-38所示。

(5) 系统自动进行电子邮件服务的安装，如图5-39所示。

(6) 安装完毕后，系统提示此服务器已经是邮件服务器，如图5-40所示。单击“完成”按钮后，邮件服务器就出现在“管理您的服务器”窗口中。

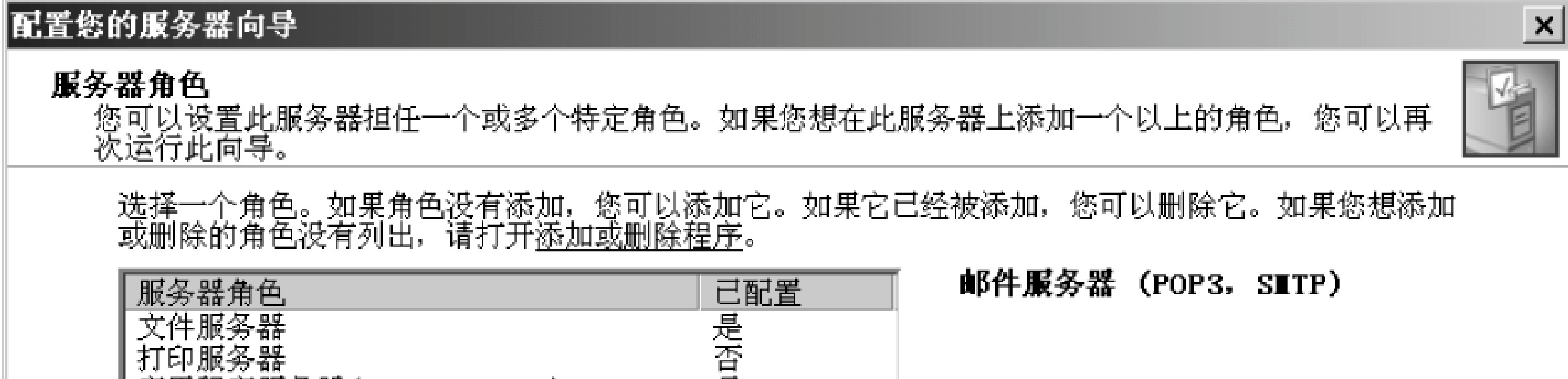


图 5-35 服务器角色选择



图 5-36 配置 POP3 服务

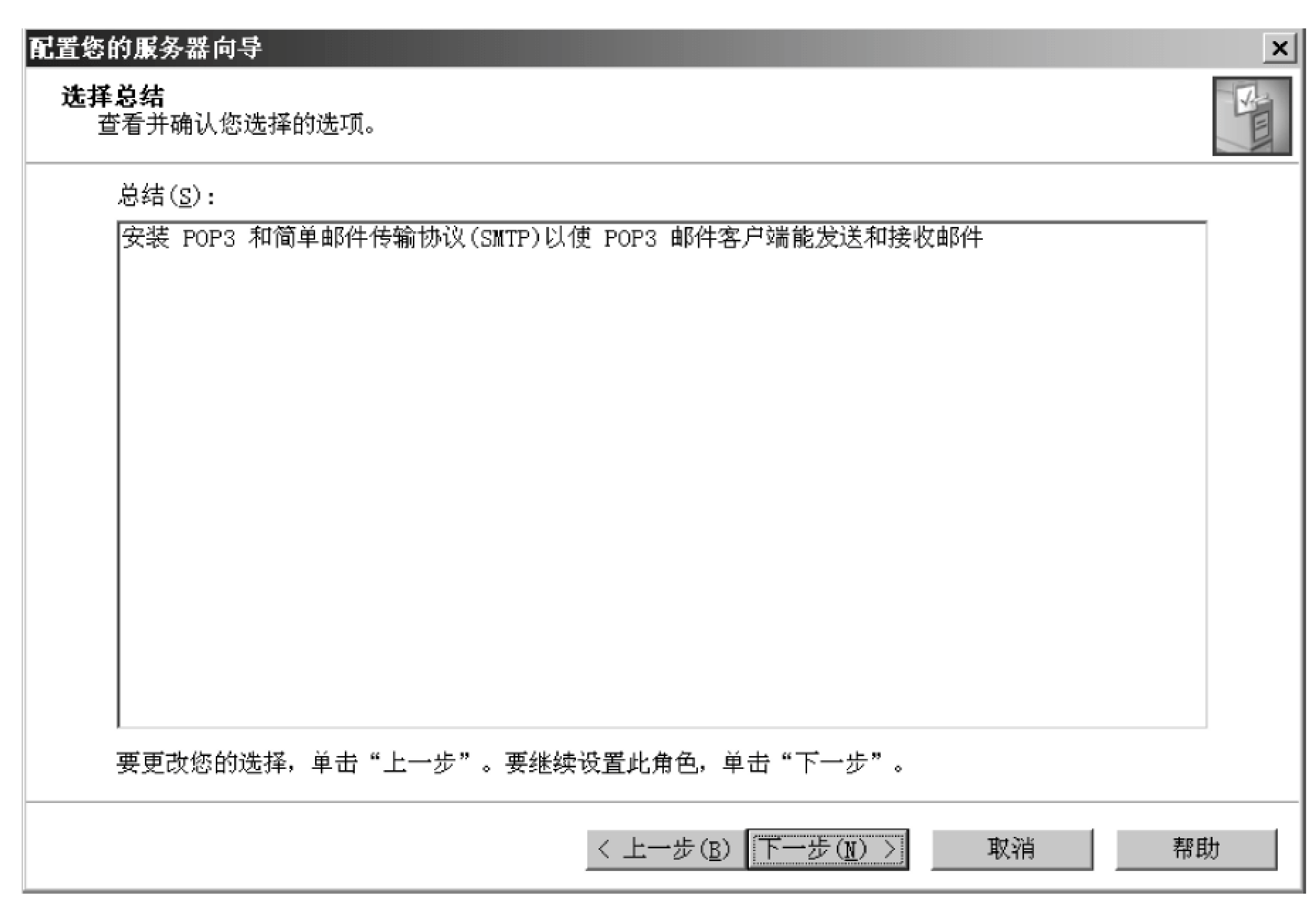


图 5-37　安装邮件服务器“选择总结”对话框

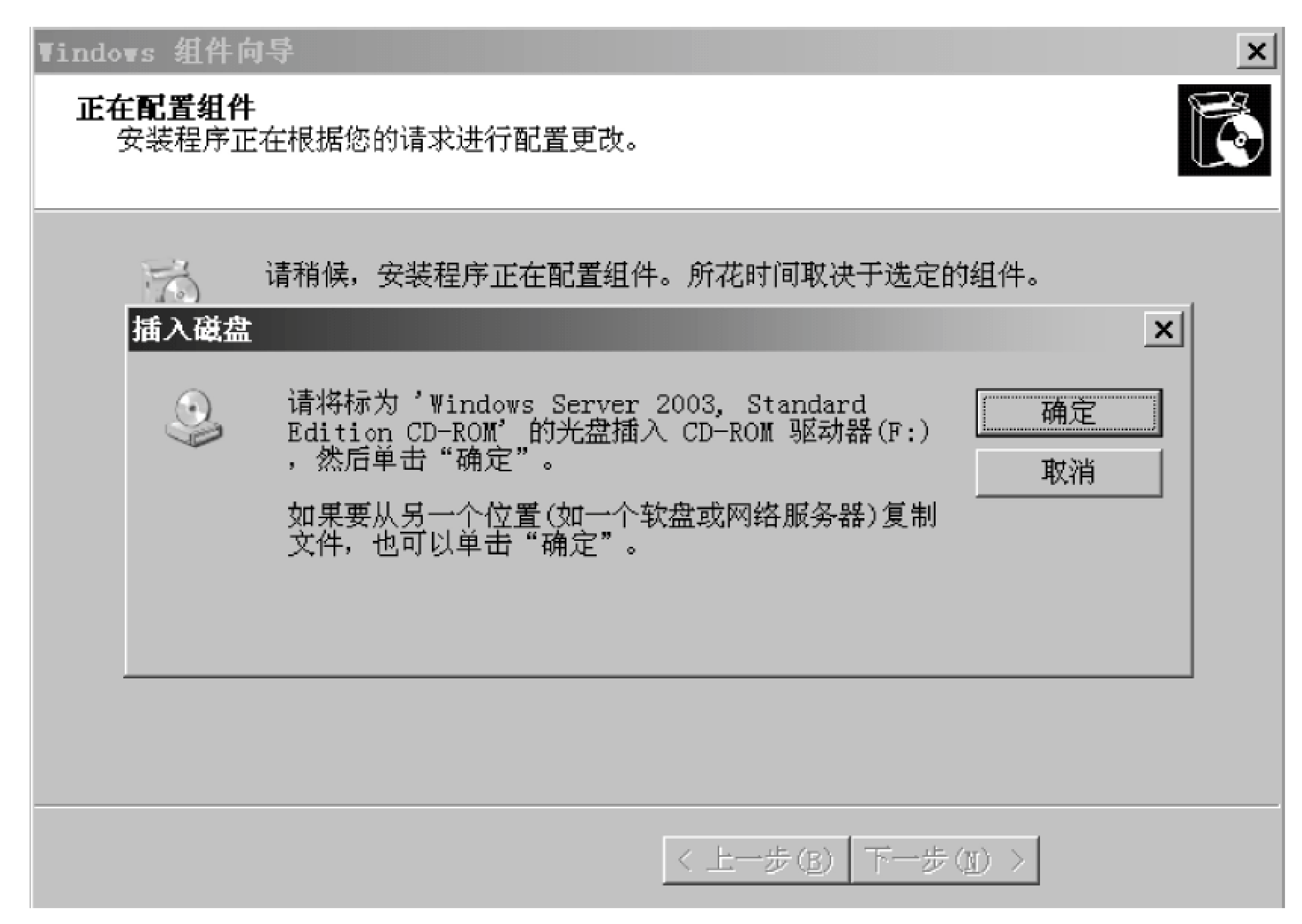


图 5-38　插入光盘



图 5-39 系统正在安装邮件服务器



图 5-40 邮件服务器安装成功

5.4.2 邮箱存储位置设置

安装完成后，系统默认状态下将用户邮件存储在 C:\Inetpub\mailroot\Mailbox 文件夹中，通常需要将邮件的存储地址修改到一个空间比较大的存储位置，但要进行这样的修改需要有足够的权限，要由 Administrator 组中的成员来进行修改。设置邮件存储位置的操作如下：

（1）在“管理您的服务器”窗口中单击“邮件服务器(POP3，SMTP)”中的“管理此邮件服务器”，系统显示“POP3 服务”控制台，如图 5-41 所示。



图 5-41 POP3 服务控制台

（2）首先停止邮件服务器。右击“POP3 服务”下的计算机名称，选择“所有任务”→“停止”。

（3）右击“POP3 服务”下的计算机名称，选择“属性”菜单，系统显示邮件服务器的属性对话框，在“根邮件目录”文本框中输入邮件存储文件夹，或单击“浏览”按钮，选择邮件存储文件夹，如图 5-42 所示。

（4）单击“确定”按钮，系统提示用户原有域无法存储邮件，需将域目录复制到新目录下，如图 5-43 所示，单击“确定”按钮。

（5）系统提示重启邮件服务器，如图 5-44 所示，单击“是”按钮。

（6）将系统默认状态下邮件存储文件夹，例如 C:\Inetpub\mailroot\Mailbox 中的域复制到新的邮件存储文件夹。

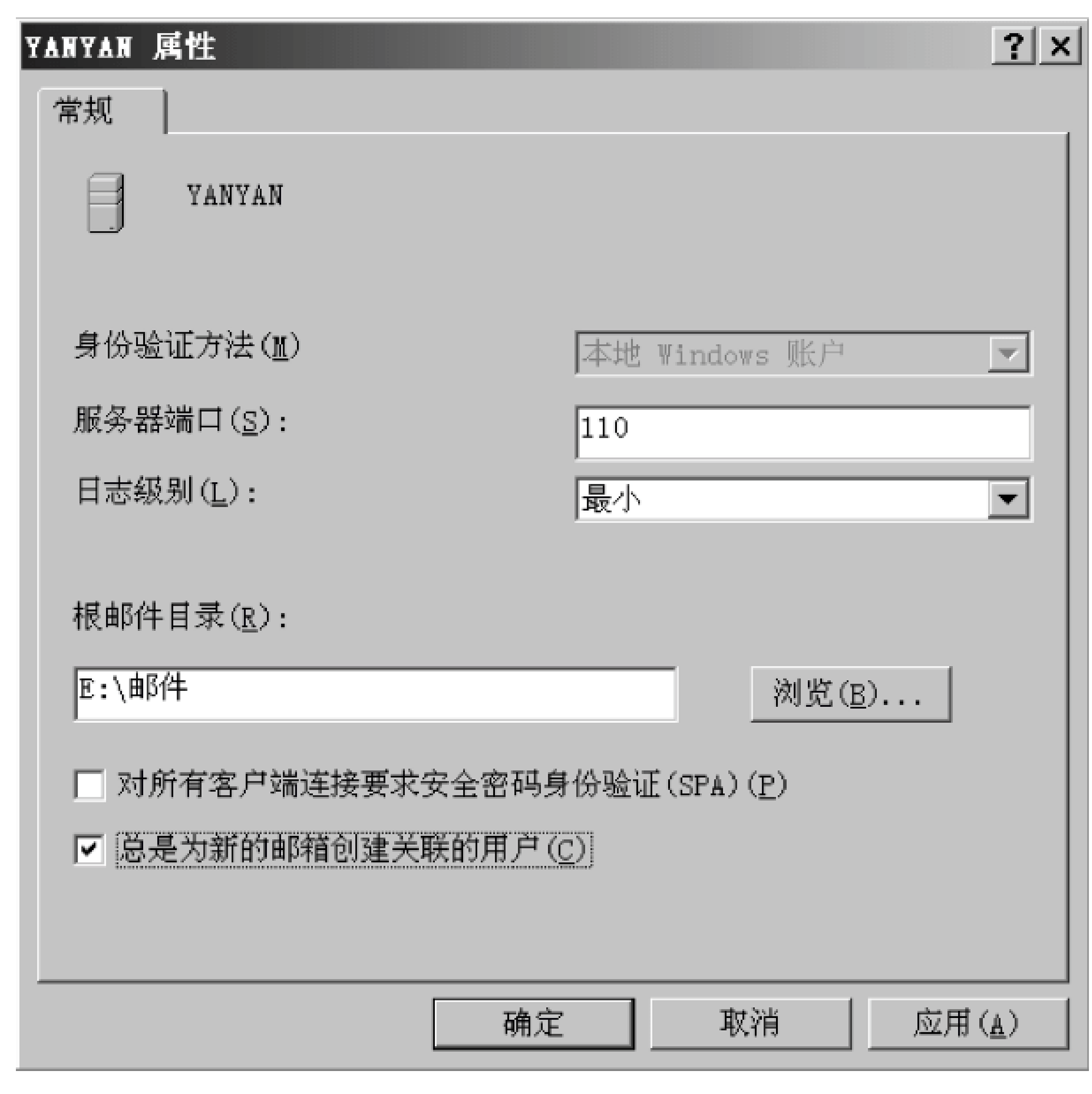


图 5-42 配置邮件服务器属性

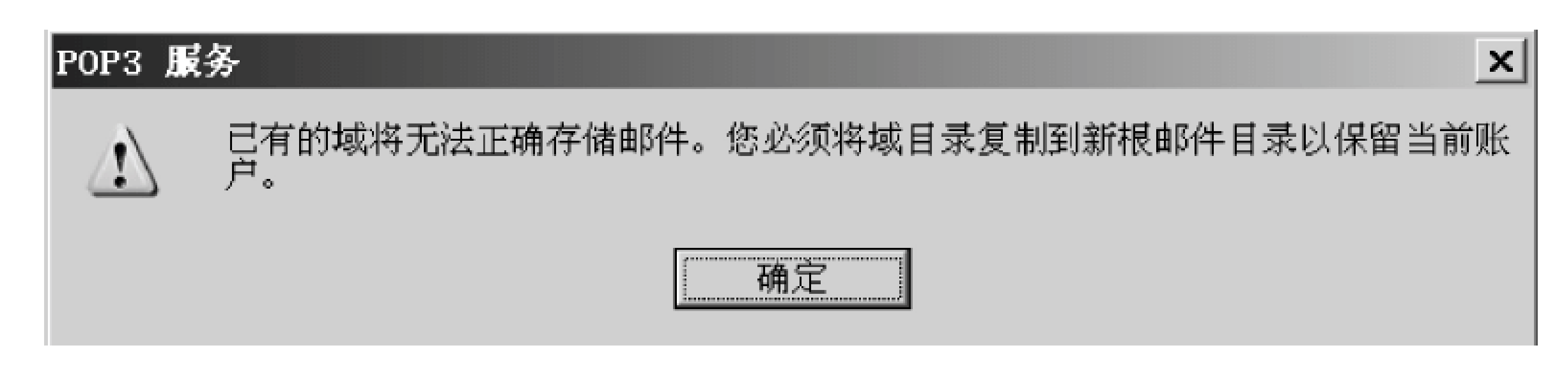


图 5-43 配置邮件服务器提示之一

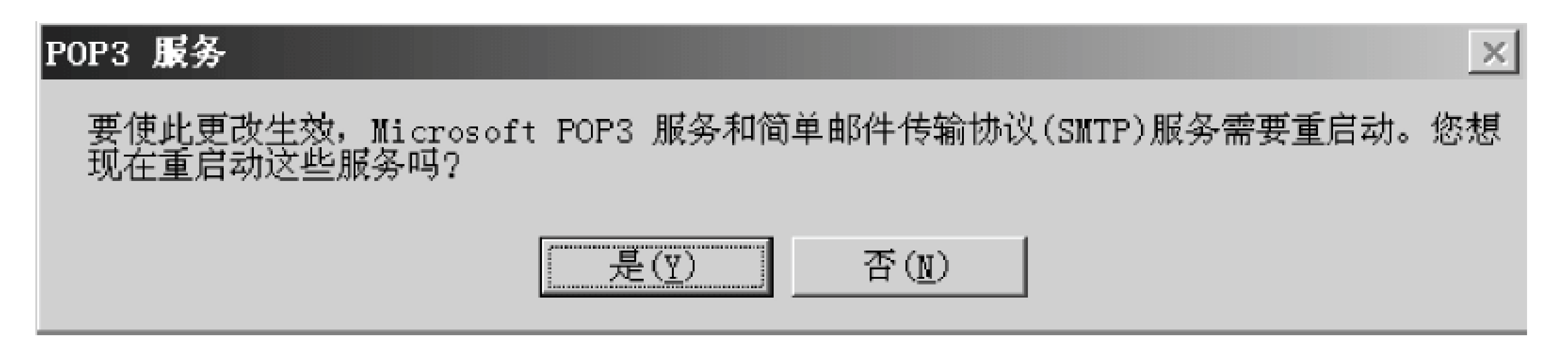


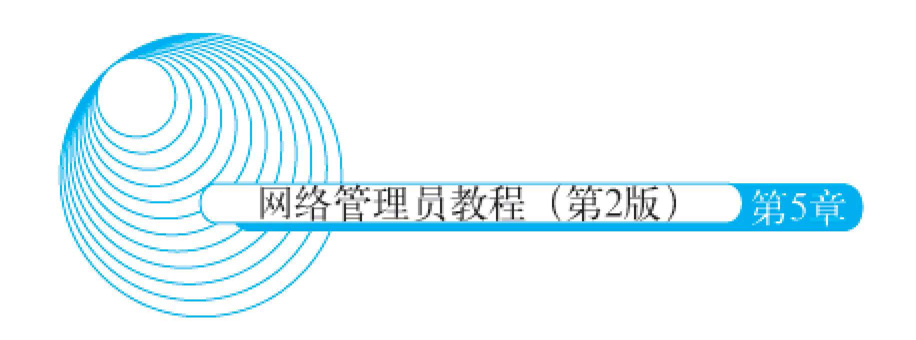
图 5-44 配置邮件服务器提示之二

(7) 右击“POP3 服务”下的计算机名称，选择“所有任务”→“重启动”，启动邮件服务。

(8) 右击“POP3 服务”下的计算机名称，选择“刷新”，使新的域目录生效。

5.4.3 域管理

邮件服务器中通过域来提供邮件服务。如果一个企业或单位需要多个域名，可以添加多个



域名实现多邮件虚拟服务共享。

1．创建域

（1）打开“POP3 服务”控制台，右击计算机名称，单击“新建”→“域”，系统显示“添加域”。

（2）在域名文本框中输入新建域的名称，如图 5-45 所示，并确保该域名已在 DNS 服务器中设置好 MX 记录。

（3）单击“确定”按钮，完成新域的添加。

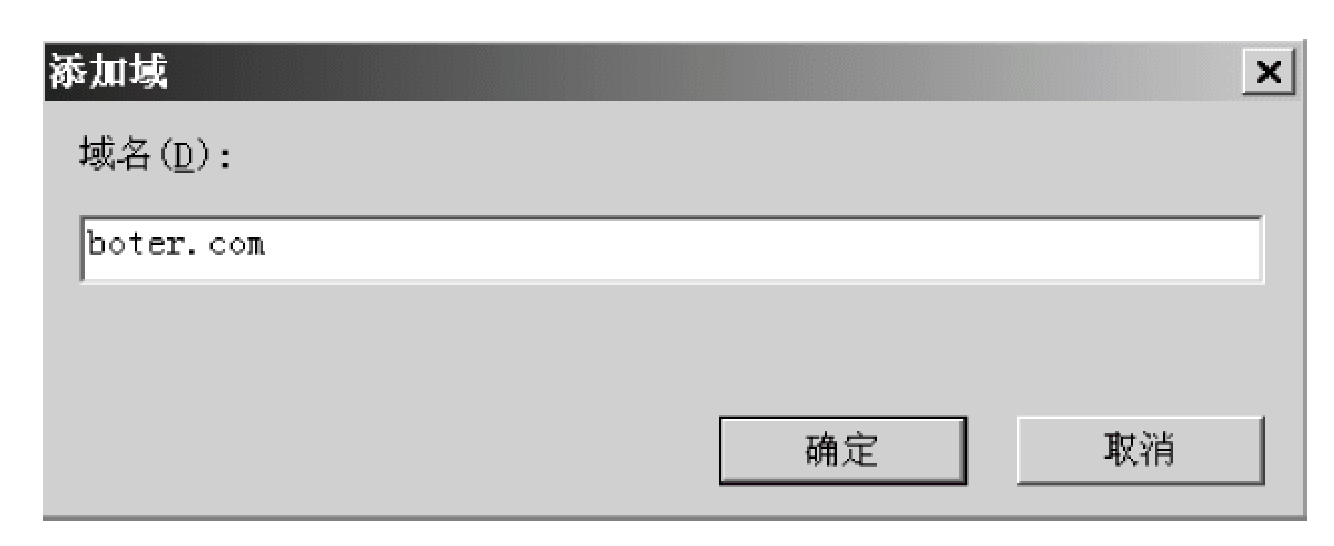


图 5-45　配置邮件服务器的域名

2．删除域

打开“POP3 服务”控制台，用鼠标右键单击要删除的域，单击“删除”按钮，然后单击“确定”按钮，即可删除该域。但是，若该域中有用户正连接到服务器，不能删除该域。

3．锁定/解除锁定域

通过锁定某个域可阻止该域的所有成员检索自己的电子邮件。

打开“POP3 服务”控制台，右击要锁定的域，即可锁定该域；同样右击要解除锁定的域，即可解除该域锁定。

5.4.4　邮箱管理

1．新建邮箱

在“POP3 服务”控制台中选中要创建新邮箱的域，右击选择“新建”→“邮箱”，出现“添加邮箱”的对话框，在文本框中分别输入“邮箱名”、“密码”、“确认密码”，单击“确定”按钮，系统提示成功添加了一个名为 leedaxing 的邮箱，如图 5-46 所示。

如图 5-47 所示，在名为 YANYAN 的服务器上，共创建了 boter.com、botertech.com 和 eqsn.gov.cn 3 个域，其中域 eqsn.gov.cn 中又创建了 zhangtao、leedaxing 和 webmaster 3 个邮箱，其中邮箱 leedaxing 的 E-mail 地址为 leedaxing@eqsn.gov.cn。



图 5-46　配置邮件服务器邮箱



图 5-47　配置邮件服务器的结果

2. 删除邮箱

在域中右击欲删除的邮箱，然后单击“删除”按钮，系统显示“删除邮箱”对话框，若要同时也删除与此邮箱相关联的用户账户则选中该复选框，单击“确定”即可删除邮箱。

此外，用户还可以根据自己的需要进行邮箱的锁定与解除锁定、邮箱属性设置等邮箱的管理操作。

5.5 配置 DHCP 服务器

DHCP 服务器是采用了动态主机配置协议（DHCP，Dynamic Host Configuration Protocol），对网络中的 IP 地址自动动态分配的服务器，旨在通过服务器集中管理网络上使用的 IP 地址和其他相关配置的详细信息，以减少管理地址配置的复杂性。

Windows Server 2003 的服务器角色中包含了 DHCP 服务器，配置方法比较简单，功能也相对单一，因篇幅所限，这里不做介绍。本节着重介绍 Red Flag Server 4.0 系统中 DHCP 服务的配置。Red Flag Server 4.0 提供了符合因特网标准草案 RFC（Request For Comments，请求注解）的 DHCP 服务，安全性和可靠性较好，不但可用于管理客户机配置并在网络上自动进行 IP 地址的指派，同时还兼有简单的网络管理功能。

5.5.1 DHCP 简介

DHCP 服务器是采用了动态主机配置协议（DHCP，Dynamic Host Configuration Protocol），对网络中的 IP 地址自动动态分配的服务器，旨在通过服务器集中管理网络上使用的 IP 地址和其他相关配置的详细信息，以减少管理地址配置的复杂性，它的前身是 BOOTP。BOOTP 原本用于无磁盘网络主机使用 BOOT ROM 而不是磁盘起动并连接上网，BOOTP 可以自动地为那些主机设定 TCP/IP 环境。但 BOOTP 有一个缺点：在设定前须事先获得客户端的硬件地址，而且与 IP 的对应是静态的。换言之，BOOTP 缺乏“动态性”，若在有限的 IP 资源环境中，BOOTP 的一对一对应会造成非常大的浪费。

DHCP 是 BOOTP 的增强版本，它分为两个部分：一个是服务器端，而另一个是客户端。所有的 IP 地址信息都由 DHCP 服务器集中管理，并负责处理客户端的 DHCP 请求；客户端使用从服务器分配下来的 IP 环境资料。DHCP 透过“租约”的概念有效且动态的分配客户端的 IP 地址。

1. DHCP 的分配形式

首先，必须至少有一台 DHCP 工作在网络上面，它会监听网络的 DHCP 请求，并与客户端协商 TCP/IP 环境设定。它提供两种 IP 定位方式：

- 自动分配（Automatic Allocation）：一旦 DHCP 客户端第一次成功的从 DHCP 服务器端租用到 IP 地址之后，就永远使用这个地址。
- 动态分配（Dynamic Allocation）：当 DHCP 第一次从 DHCP 服务器端租用到 IP 地址之

后，并非永久的使用该地址，只要租约到期，客户端就得释放(release)这个 IP 地址，以给其他工作站使用。当然，客户端可以比其他主机更优先的延续(renew)租约，或是租用其他的 IP 地址。

动态分配显然比自动分配更加灵活，尤其是当实际 IP 地址不足的时候。例如：一家 ISP 只能提供 200 个 IP 地址用来给拨接客户，但并不意味着客户最多只能有 200 个。因为，客户们不可能全部同一时间上网，除了他们各自的行为习惯的不同，也有可能是电话线路的限制。这样就可以将这 200 个地址，轮流地租用给拨接上来的客户使用了。

DHCP 除了能动态的设定 IP 地址之外，还可以将一些 IP 保留下来给一些特殊用途的机器使用，它可以按照硬件位置来固定地分配 IP 地址，这样可以给用户更大的设计空间。同时，DHCP 还可以帮客户端指定 router 、 netmask 、 DNS Server 、 WINS Server 等项目。

2. DHCP 的工作原理

区别于客户端是否第一次登录网络，DHCP 的工作形式会有所不同。

1) 第一次登录

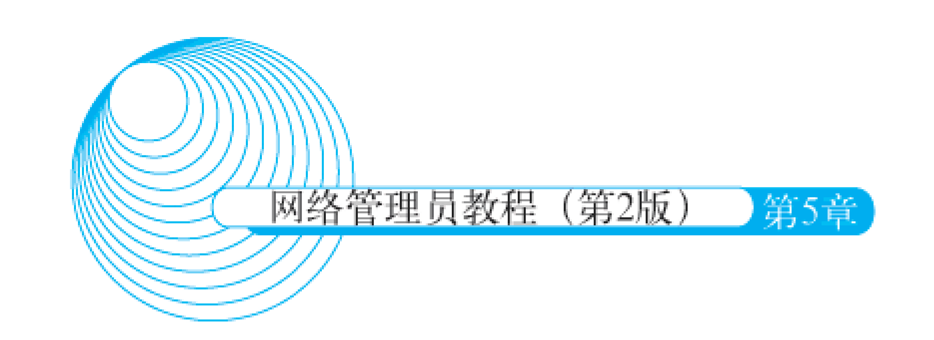
(1)寻找 Server。当 DHCP 客户端第一次登录网络的时候，也就是客户发现本机上没有任何 IP 资料设定，它会向网络发出一个 Dhcpdiscover 包。因为客户端还不知道自己属于哪一个网络，所以包的来源地址会为 0.0.0.0 ，而目的地址则为 255.255.255.255 ，然后再附上 Dhcpdiscover 的信息，向网络进行广播。

在 Windows 的预设情形下，Dhcpdiscover 的等待时间预设为 1 秒，也就是当客户端将第一个 Dhcpdiscover 包送出去之后，在 1 秒之内没有得到回应的话，就会进行第二次 Dhcpdiscover 广播。在一直得不到回应的情况下，客户端一共会有 4 次 Dhcpdiscover 广播，除了第一次会等待 1 秒之外，其余 3 次的等待时间分别是 9 、 13 、 16 秒。如果都没有得到 DHCP 服务器的回应，客户端则会显示错误信息，宣告 Dhcpdiscover 的失败。之后，基于使用者的选择，系统会继续在 5 分钟之后再重复一次 Dhcpdiscover 的过程。

(2) 提供 IP 租用地址。当 DHCP 服务器监听到客户端发出的 Dhcpdiscover 广播后，它会从那些还没有租出的地址范围内，选择最前面的闲置 IP ，连同其他 TCP/IP 设定，回应给客户端一个 Dhcpoffer 包。

由于客户端最初并没有 IP 地，所以在其 Dhcpdiscover 封包内会带有其 MAC 地址信息，并且有一个 XID 编号来辨别该封包，DHCP 服务器回应的 Dhcpoffer 封包则会根据这些资料传递给要求租约的客户。根据服务器端的设定，Dhcpoffer 封包会包含一个租约期限的信息。

(3) 接受 IP 租约。如果客户端收到网络上多台 DHCP 服务器的回应，只会挑选其中一个 Dhcpoffer 而已(通常是最先抵达的那个)，并且会向网络发送一个 Dhcprequest 广播封包，告诉所有 DHCP 服务器它将指定接受哪一台服务器提供的 IP 地址。



同时，客户端还会向网络发送一个 ARP 封包，查询网络上面有没有其他机器使用该 IP 地址；如果发现该 IP 已经被占用，客户端则会送出一个 Dhcpdeclinf 封包给 DHCP 服务器，拒绝接受其 Dhcpoffer，并重新发送 Dhcpdiscover 信息。

事实上，并不是所有 DHCP 客户端都会无条件接受 DHCP 服务器的 offer，尤其这些主机安装有其他 TCP/IP 相关的客户软件。客户端也可以用 Dhcprequest 向服务器提出 DHCP 选择，而这些选择会以不同的号码填写在 DHCP Option Field 里面。换一句话说，在 DHCP 服务器上面的设定，未必是客户端全都接受，客户端可以保留自己的一些 TCP/IP 设定。而主动权永远在客户端这边。

（4）租约确认。当 DHCP 服务器接收到客户端的 Dhcprequest 之后，会向客户端发出一个 Dhcpack 回应，以确认 IP 租约的正式生效，也就结束了一个完整的 DHCP 工作过程。

以上的工作流程如图 5-48 所示。

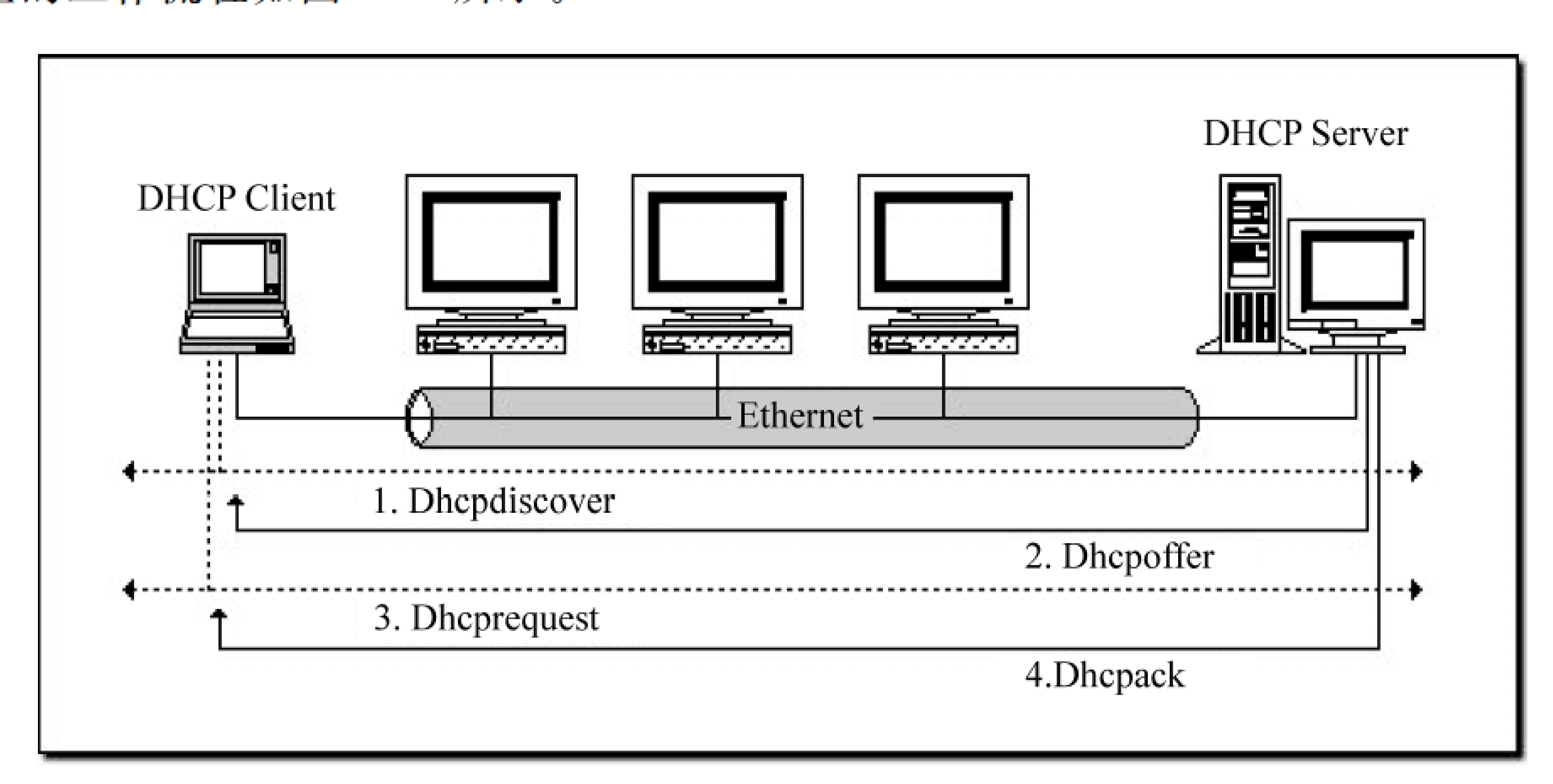


图 5-48 DHCP 的工作流程

2）非第一次登录

一旦 DHCP 客户端成功地从服务器取得 DHCP 租约之后，除非其租约已经失效并且 IP 地址重新设定回 0.0.0.0，否则就无需再发送 Dhcpdiscover 信息了，而会直接使用已经租用到的 IP 地址向之前的 DHCP 服务器发出 Dhcprequest 信息，DHCP 服务器会尽量让客户端使用原来的 IP 地址，如果没问题的话，直接回应 Dhcpack 来确认即可。如果该地址已经失效或已经被其他机器使用了，服务器则会回应一个 Dhcpnack 封包给客户端，要求其从新执行 Dhcpdiscover。

5.5.2 DHCP 服务器的管理

Windows Server 2003 的服务器角色中包含了 DHCP 服务器，配置方法比较简单，功能也相对单一，因篇幅所限，这里不做介绍。本节着重介绍 Red Flag Server 4.0 系统中 DHCP 服务的

配置。Red Flag Server 4.0 提供了符合 RFC(request for comment,请求评论[文档])的 DHCP 服务,安全性和可靠性较好,不但可用于管理客户机配置并在网络上自动进行 IP 地址的指派,同时还兼有简单的网络管理功能。

Red Flag Server 4.0 中,DHCP 服务器的管理配置,主要使用图形化配置工具 fdhcp 管理服务器、共享网络、子网、主机以及群组。rfdhcp 可以对服务器的大部分功能进行配置。对于配置工具不支持的功能,可以利用工具中提供的编辑器对 DHCP 配置文件进行手工编辑。

1. 打开 DHCP 配置工具

可以采用以下方法启动 rfdhcp 工具:

- 在系统主菜单中选择“系统”→“控制面板”,打开控制面板,在“网络服务配置”标签页中,双击“DHCP 配置工具”。
- 在系统主菜单中选择“管理工具”→“DHCP 配置工具”。
- 在运行命令行或 shell 提示符下直接输入 rfdhcp。

2. 启动和停止 DHCP 服务

打开 rfdhcp 配置工具,在主窗口左侧的控制台树中,单击相应的 DHCP 服务器。

- 要启动 DHCP 服务,在菜单中选择“操作”→“所有任务”→“开始”。
- 要停止 DHCP 服务,在菜单中选择“操作”→“所有任务”→“停止”。
- 要重新启动 DHCP 服务,在菜单中选择“操作”→“所有任务”→“重新开始”。

也可以在命令行终端下,通过下列命令执行这些任务:

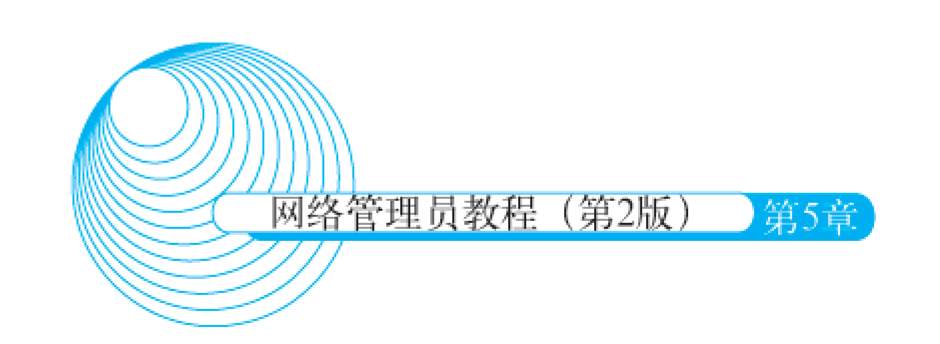
```
# /etc/rc.d/init.d/dhcpd start
# /etc/rc.d/init.d/dhcpd stop
# /etc/rc.d/init.d/dhcpd restart
```

3. 查看 DHCP 服务器的属性

打开 rfdhcp 配置工具,在主窗口左侧的控制台树中,单击相应的 DHCP 服务器。选择菜单中的“操作”→“属性”,打开“DHCP 属性”对话框,根据需要查看或修改服务器的属性。

4. 授权 DHCP 服务器

DHCP 服务器在网络上正确配置和授权使用时,将提供有用且计划好的管理服务。但是,当错误配置或未授权的 DHCP 服务器被引入网络时,可能会产生问题。例如,如果启动了未授权的 DHCP 服务器,它可能开始为客户机租用不正确的 IP 地址或者否认尝试更新当前地址租约的 DHCP 客户机。这些配置中的任何一个错误都可能导致启用 DHCP 的客户机产生更多的



问题。例如，从未授权的服务器获取配置租约的客户机找不到有效的域控制器，致使客户机难以成功登录到网络。为避免出现这些问题，在它们为客户提供服务之前，请在网络中验证服务器是否合法。这样就避免了由于在错误网络上运行带有不正确配置的 DHCP 服务器。

网络上运行的权威 DHCP 服务器将通知配置错误的 DHCP 客户机更新其配置。如果要指定一台 DHCP 服务器为权威服务器，在服务器的“属性”对话框中选择“授权此服务器为网络上的权威服务器”。

需要指出的是，只有网络管理员才可以选择“授权此服务器为网络上的权威服务器”。如果不能确定自己是否具有网络管理员身份，请不要选择上述选项。

5.5.3 子网的管理

子网是对使用 DHCP 服务的子网进行的计算机管理性分组。管理员首先为每个物理子网创建子网，然后使用该子网定义由客户机使用的参数。

1. 创建新子网

(1) 打开 rfdhcp 工具，在主窗口左侧的控制台树中，单击相应的 DHCP 服务器、共享网络或群组。在菜单中选择“操作”→“新建子网”，或者右击从快捷菜单中选择“新建子网”，也可以单击工具栏中的“新建子网”按钮，弹出“新建子网向导”。在欢迎界面中，单击“下一步”按钮继续，出现如图 5-49 所示的“子网 ID 与掩码”设置界面。

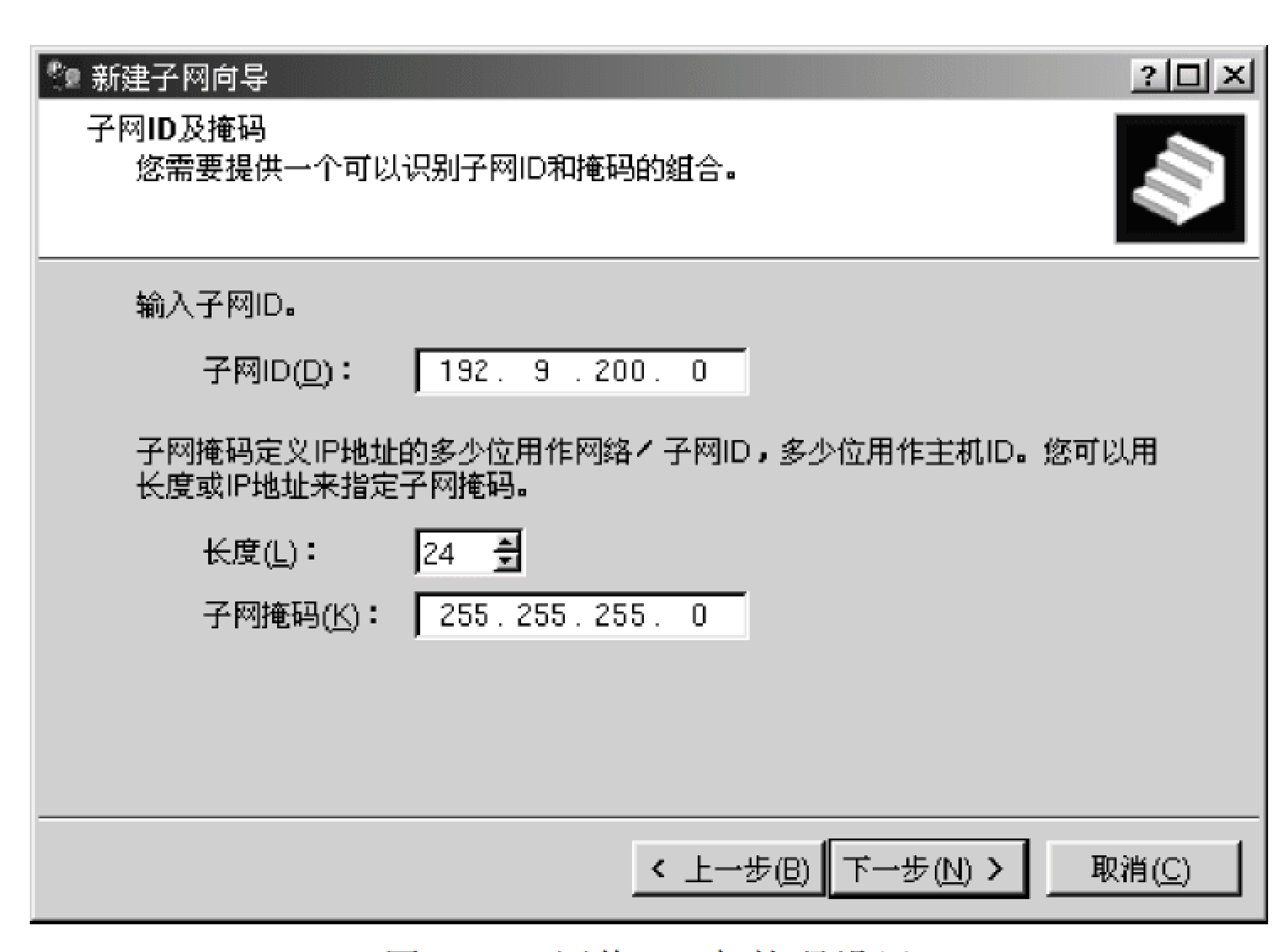


图 5-49　网络 ID 与掩码设置

(2) 在“网络 ID”中输入新建子网的网络标识，“长度”和“子网掩码”中会自动出现对应的数据，可以根据需要修改。单击“下一步”按钮，则出现规划发放的 IP 地址范围对话框，如图 5-50 所示。在此可以通过输入“起始 IP 地址”和“结束 IP 地址”来确定多个连续的 IP 地址范围。如果要添加一个单独的地址，则只在“起始 IP 地址”中输入数值即可。每设置一个 IP 地址范围后，单击“添加”按钮，将其加入地址范围列表中。

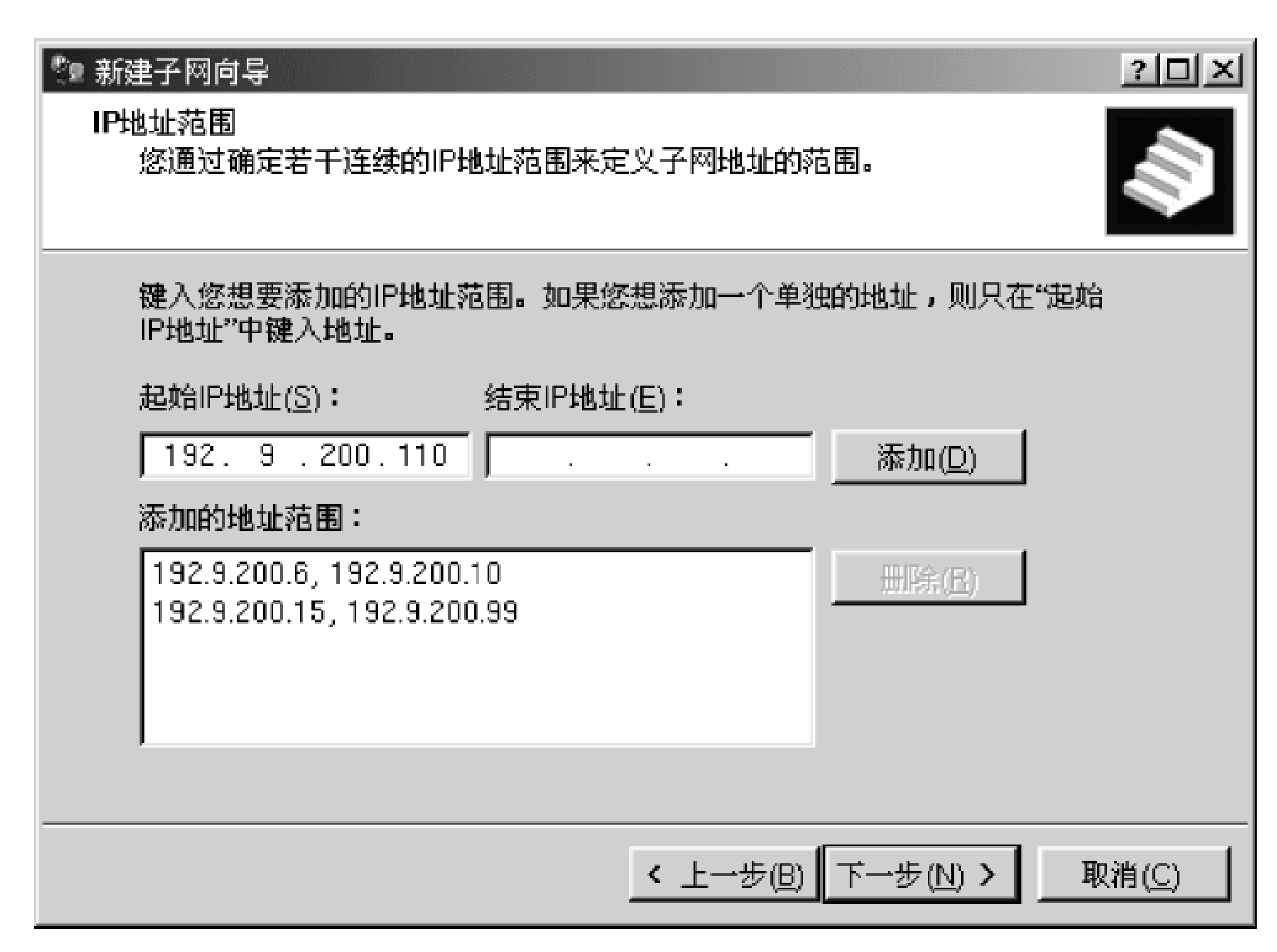


图 5-50　规划 IP 地址范围

(3) 单击“下一步”按钮，设置客户端得到 IP 地址的租约时间长度。一般而言，对于一个变动性较高的局域网，就要设置较短的租约期限；而对于一个主要包含台式计算机，位置固定的网络来说，就设置较长的租约期限。如图 5-51 所示。

(4) 单击“下一步”按钮，出现如图 5-52 所示界面，这时已经设置了一个基本的子网。向导提示配置常用的 DHCP 选项以使用新建的子网。如果不打算设置这些选项，可以单击“否，我想稍后配置这些选项”。这些选项可以在“子网选项”中进行设置。依照默认的选择“是，我想现在配置这些选项”，单击“下一步”按钮。

(5) 随后出现如图 5-53 所示的“路由器(默认网关)设置”对话框。在“IP 地址”栏中输入为子网分配的路由器或默认网关的 IP 地址，然后单击“添加”按钮。也可以输入服务器名称后，单击“解析”按钮，让系统自动寻找其 IP 地址。如果没有预设的路由器或网关，则不必输入任何数据。

(6) 单击“下一步”按钮，进入“域名称和 DNS 服务器”设置界面，如图 5-54 所示。在“IP 地址”栏中输入子网上的计算机进行 DNS 名称解析时使用的父域；如果有 DNS 服务器，输入其名

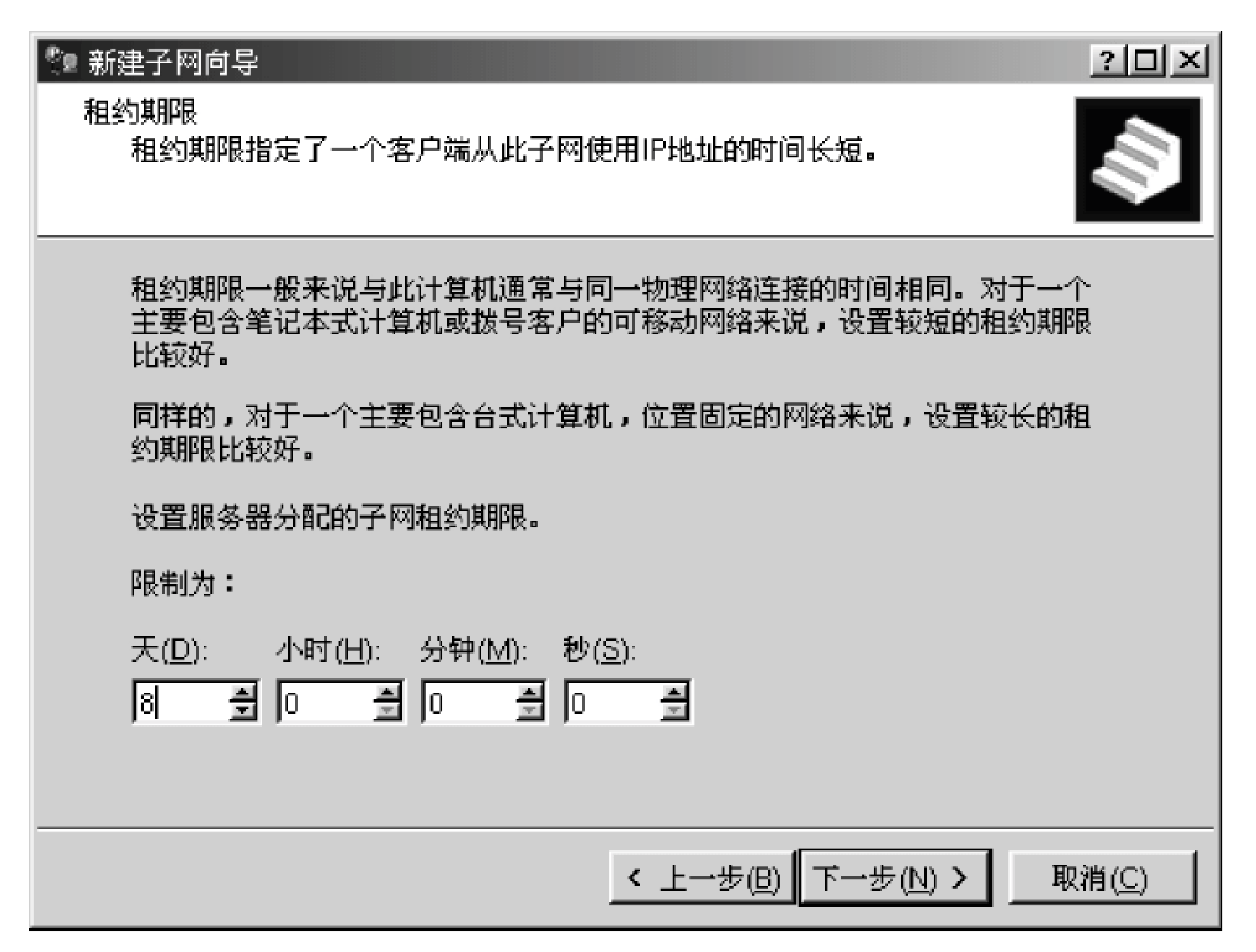


图 5-51　设置租约期限

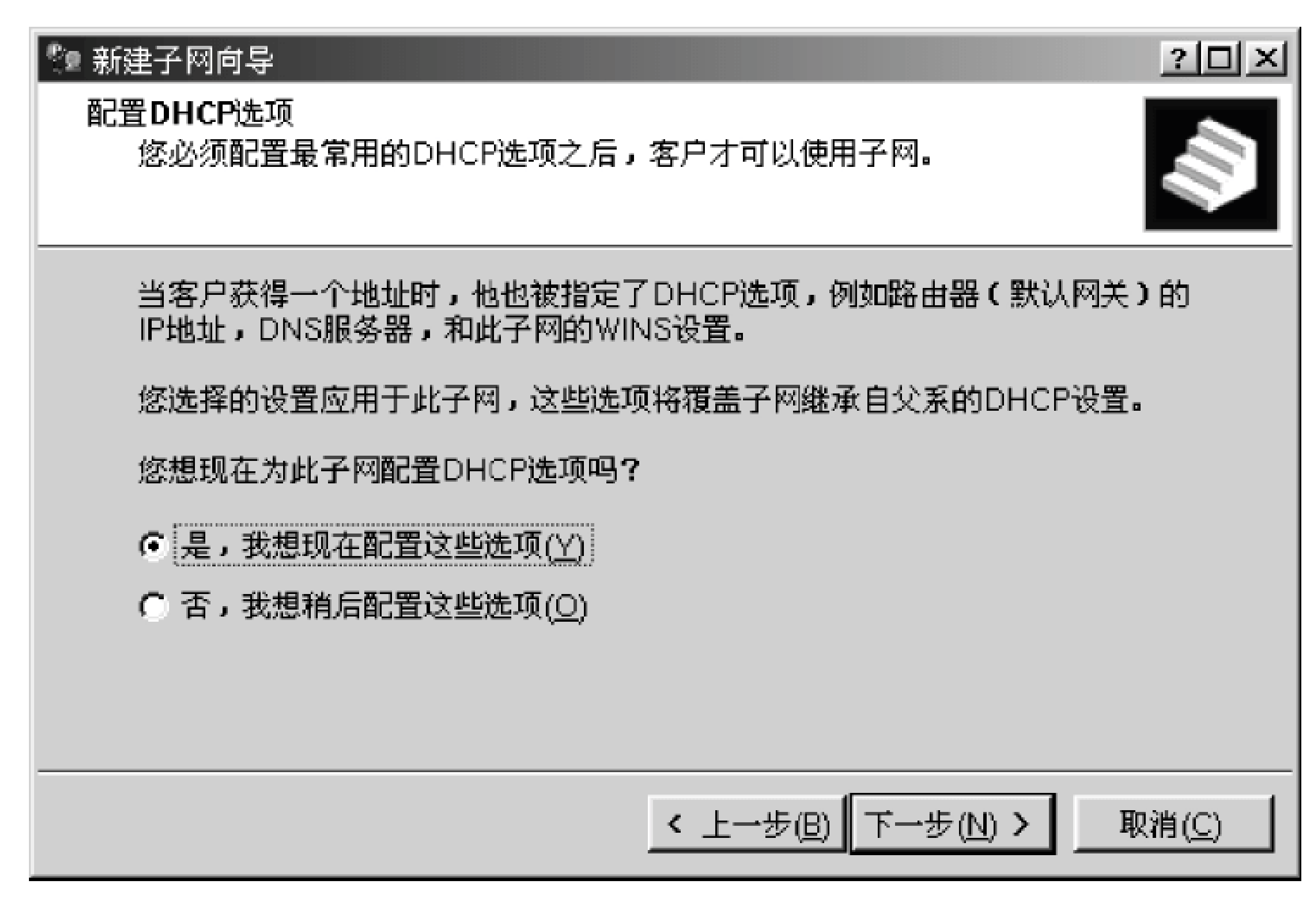


图 5-52　配置选项

称或 IP 地址后单击“添加”按钮，也可以输入服务器的名称后，单击“解析”按钮让系统自动寻找其 IP 地址。

（7）单击“下一步”按钮，进行 WINS 服务器的相关设置，如图 5-55 所示。设置方法同上。

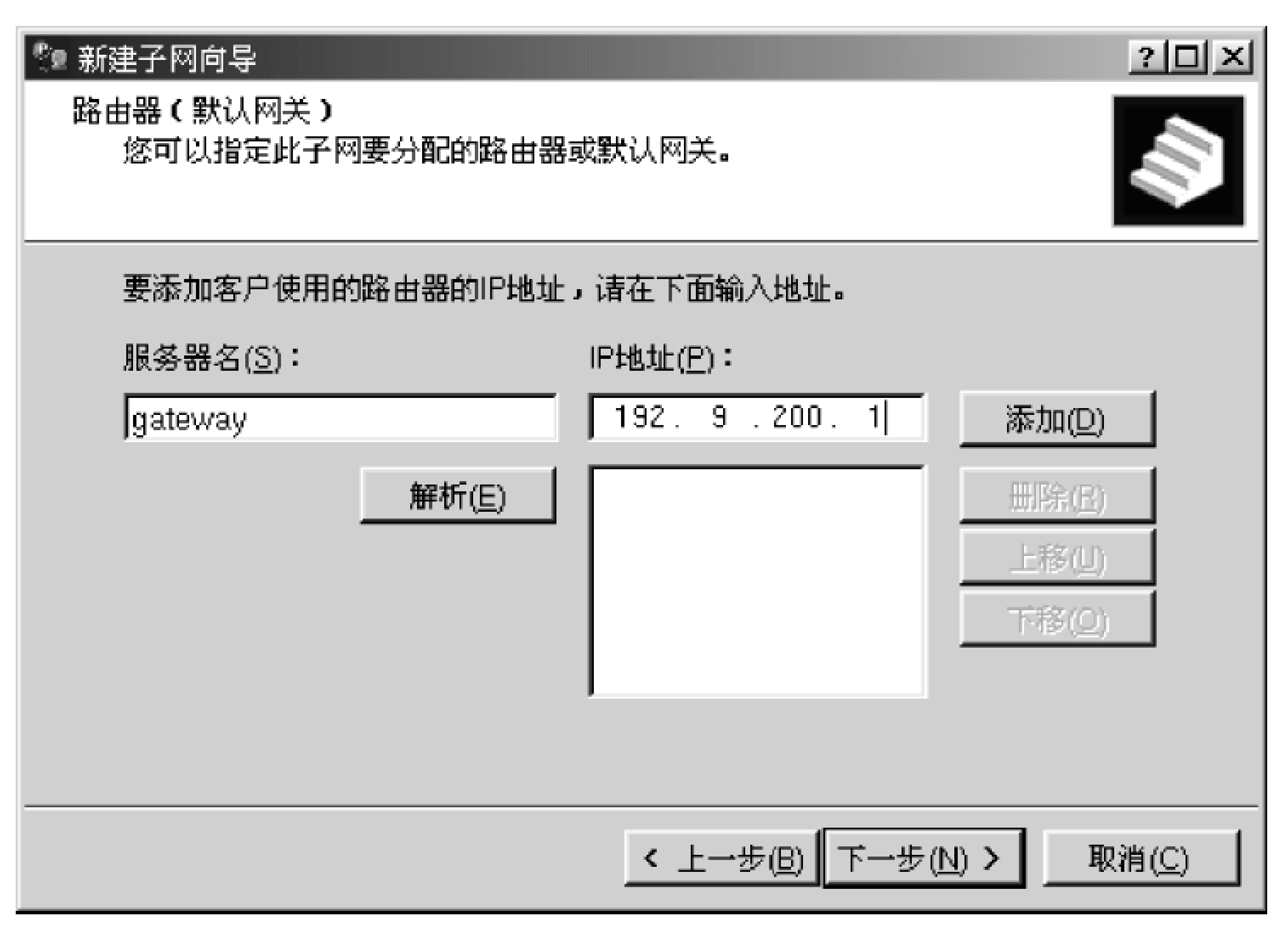


图 5-53　设置路由和网关

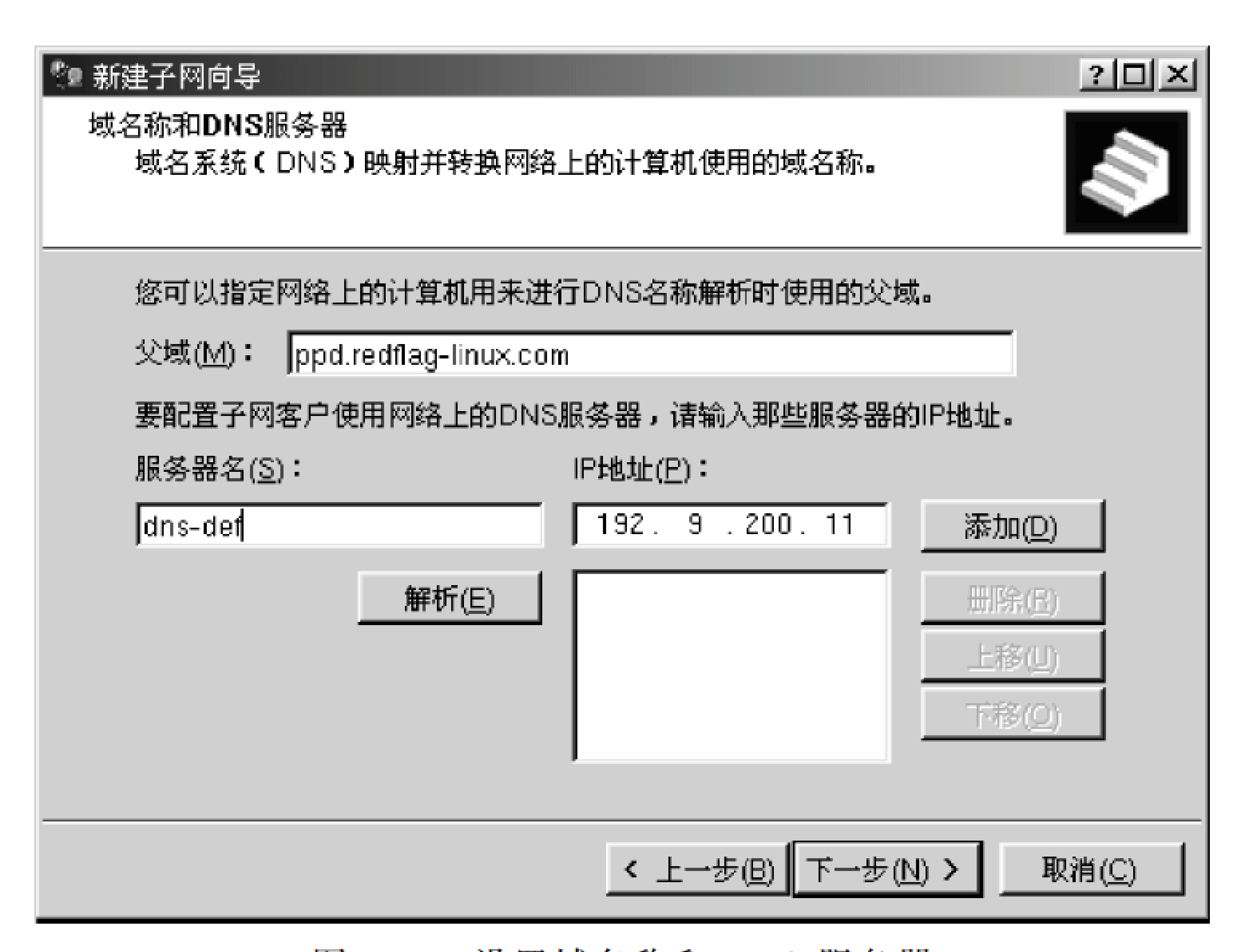


图 5-54　设置域名称和 DNS 服务器

完成此步骤后，单击“下一步”按钮，出现完成新建子网向导界面。重新启动 dhcpd 服务后，客户端就可以使用这个子网中的地址了。

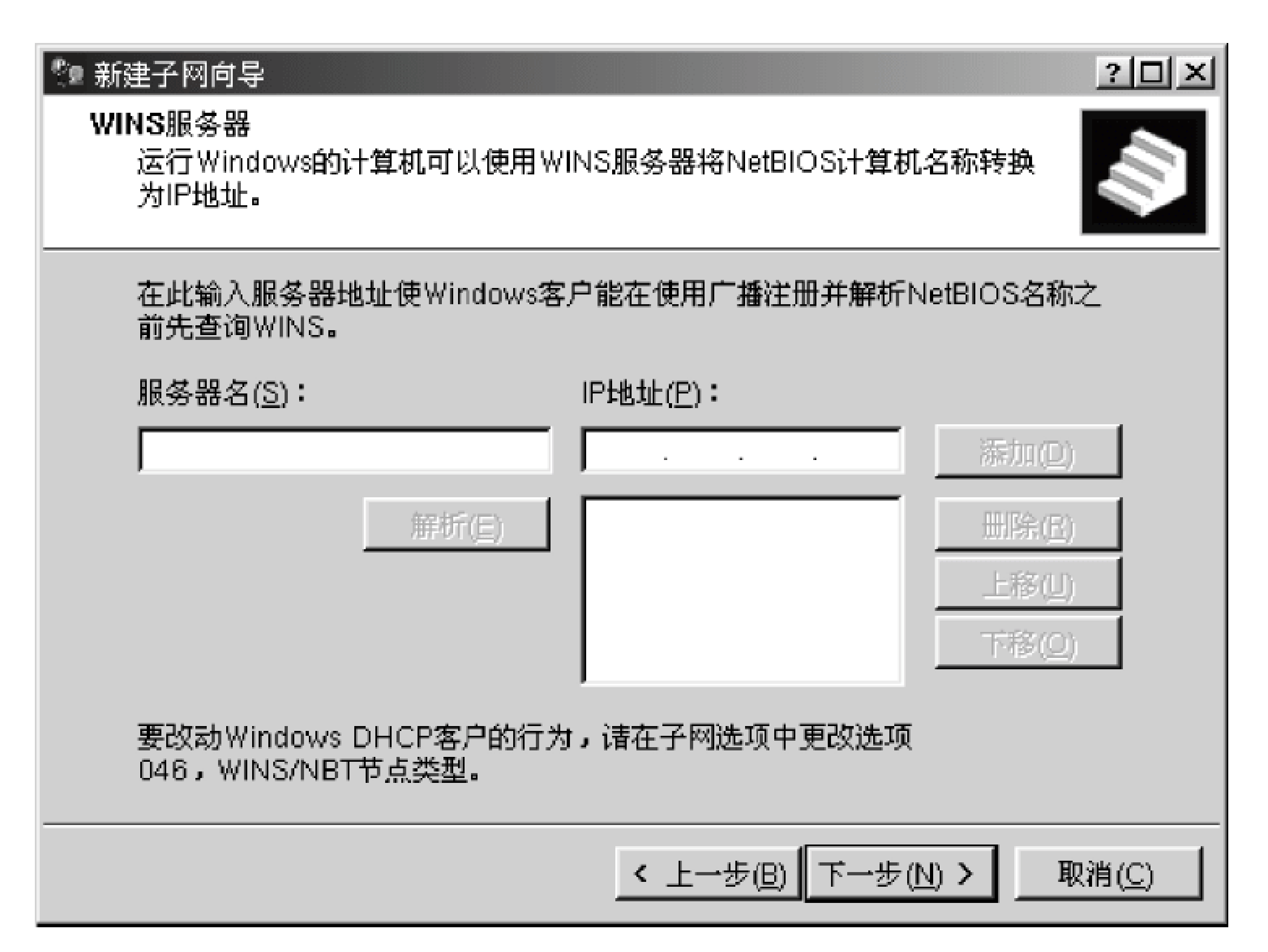


图 5-55　设置 WINS 服务器

2. 向子网中加入地址范围

子网中定义的地址范围中所包含的地址应该是由 DHCP 服务器向从该子网获得租约的客户机提供的。具体添加方法如下：

(1) 在 rfdhcp 配置工具主窗口左侧的控制台树中，展开相应的子网，选择“地址池”选项。单击菜单中的“操作”→“新建地址范围”，也可以右击选择快捷菜单的“新建地址范围”菜单项。

(2) 在“新建地址范围”对话框中，输入要向该子网中添加的 IP 地址范围的“起始 IP 地址”和“结束 IP 地址”。如果只要添加一个单独的地址，则只输入“起始 IP 地址”即可。

(3) 如果希望服务器将这个范围内的地址动态分配给 BOOTP 客户，请选中“允许 BOOTP 客户”。

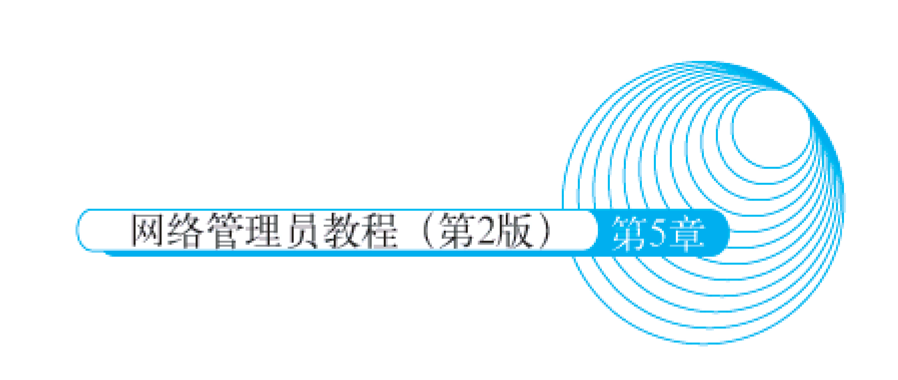
(4) 单击“添加”按钮，新增的地址范围将显示在主窗口右侧的地址池列表中。

3. 更改或查看子网属性

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的子网。单击菜单中的“操作”→“属性”，也可以右击选择快捷菜单中的“属性”菜单项。打开“子网属性”对话框，可以根据需要查看或修改子网的属性。

关于子网，有下列属性：

(1) 唯一的子网 ID 识别码，用于子网的身份鉴别。



（2）唯一的子网掩码，用于确定给定 IP 地址的子网。

（3）租约期限，它将指派给动态接收分配的 IP 地址的 DHCP 客户机。

4. 查看客户机租约信息

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应子网的“地址租约”项。在窗口右侧的详细信息列表中，可以查看客户机的租约信息。

5. 删除子网

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，单击相应的子网。选择菜单中的“操作”→“删除”。出现提示时，请确认是否删除该子网。

5.5.4 共享网络的管理

共享网络是可以通过 DHCP 配置工具创建和管理的 DHCP 服务器的一种管理功能。使用共享网络，可以将多个子网组合为单个管理实体。使用此功能，DHCP 服务器可以：

（1）在使用多个逻辑 IP 网络的单个物理网段（如单个以太网的局域网段）支持 DHCP 客户机。在每个物理子网或网络上使用多个逻辑 IP 网络时，这种配置通常被称为“多网”。

（2）支持位于 DHCP 和 BOOTP 中继代理远端的远程 DHCP 客户机，而在中继代理远端的网络上使用多网配置。

（3）在多网配置中，可以使用 DHCP 共享网络来组合并激活网络上使用的单独子网范围内的 IP 地址。

1. 创建共享网络

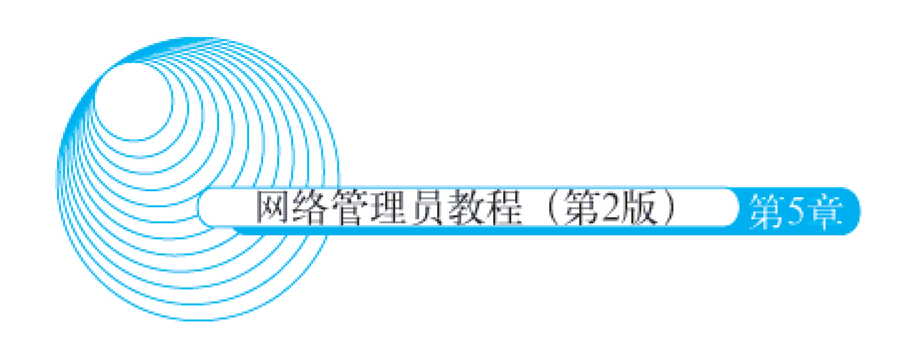
在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的 DHCP 服务器或群组。单击菜单中的“操作”→“新建共享网络”，也可以右击选择快捷菜单中的“新建共享网络”菜单项。在“新建共享网络向导”中，按提示信息完成操作。

该菜单项只有在用户至少已经在服务器或群组中创建了一个子网，而且该子网目前不是共享网络或其他群组的一部分时才显示。共享网络中包含的子网有时称作“成员子网”。可以在创建期间或在创建以后将子网添加至共享网络中。

2. 将子网添加到共享网络

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的子网。用鼠标将子网拖动到希望加入的共享网络中。出现提示时，单击“是”按钮完成子网移动。

为完成此过程，在相应的 DHCP 服务器上必须至少已存在一个共享网络。另外，无法移动



共享网络中唯一的子网。

3. 删除共享网络

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的共享网络。单击菜单中的“操作”→“删除”，也可以右击在快捷菜单中选择“删除”。出现提示时，请确认是否删除该共享网络。

删除共享网络会删除所有包含在其中的成员子网、主机、群组。如果想保留某个成员，请在删除共享网络之前先将它移到服务器或其他共享网络中。

5.5.5 主机的管理

使用主机保留地址，可以将特定的 IP 地址分配给特定的 DHCP 客户机使用。此外也可以通过主机将一组固定的设置参数提供给指定的某些网络客户机。

1. 添加主机

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应子网的“保留”项。单击菜单中的“操作”→“新建主机”，也可以在右键快捷菜单中选择“新建主机”。

在“新建主机”对话框中，输入要保留的客户机名称与 IP 地址，还有客户机的 MAC 地址。填完后单击“添加”按钮，如果不再增加其他保留地址，则单击“关闭”按钮结束。相应的主机将添加到该子网中。

关于保留主机，有以下几点说明：

(1) 也可以在服务器、共享网络、群组和子网保留中添加主机。

(2) 可以明确指定主机的 IP 地址；也可以不添加任何地址，由 DHCP 服务器动态为客户机分配地址。

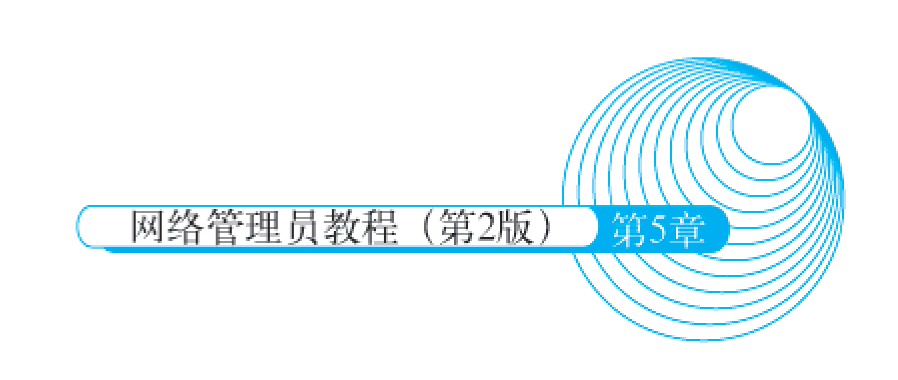
(3) 主机硬件一般是在相应网络连接的 DHCP 客户机媒体访问控制(MAC)地址的基础上确认的。除以太网外，DHCP 服务器也支持令牌环硬件类型，但暂不支持 FDDI 硬件。

(4) DHCP 服务器通过客户发送的唯一客户机识别码来确认客户，这个识别码由常规选项“061 唯一客户机识别码”来确定。如果这个识别码没有被定义，则需要通过对方的媒体访问控制(MAC)地址来识别主机客户。

2. 更改或查看主机属性

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，选择相应的主机。单击菜单中的“操作”→“属性”，也可以右击选择快捷菜单中的“属性”项。

打开主机属性对话框，可以根据需要查看或修改主机的属性。



3．删除主机

打开 rfdhcp 工具，在主窗口左侧的控制台树中，选择相应主机。单击菜单中的“操作”→“删除”，也可以右击选择快捷菜单中的“删除”项。出现提示时，请确认是否删除该主机。

5.5.6 群组的管理

使用群组，可以将多个子网、共享网络、主机组合为单个管理实体。对于群组成员没有定义的参数设置，DHCP 服务器会自动应用成员所属群组中的参数定义值。

1．创建群组

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，选择相应的 DHCP 服务器、共享网络、子网或者群组。单击菜单中的“操作”→“新建群组”，也可以右击选择快捷菜单中的“新建群组”项。在“新建群组向导”中，按提示信息完成操作。

需要说明的是，该菜单选项只有在用户至少已经在所选节点中创建了一个共享网络、子网或者主机（它目前不是共享网络或其他群组的一部分）时显示。另外，群组可在创建期间或在创建以后将子网、主机、共享网络或者其他群组添加至其中。

2．添加成员到群组中

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，选择希望添加入群组的成员节点，群组成员可以是子网、主机、共享网络或者其他的群组。用鼠标将目标成员拖动到目的群组中，出现提示时，单击“是”按钮，移动该节点。

3．删除群组

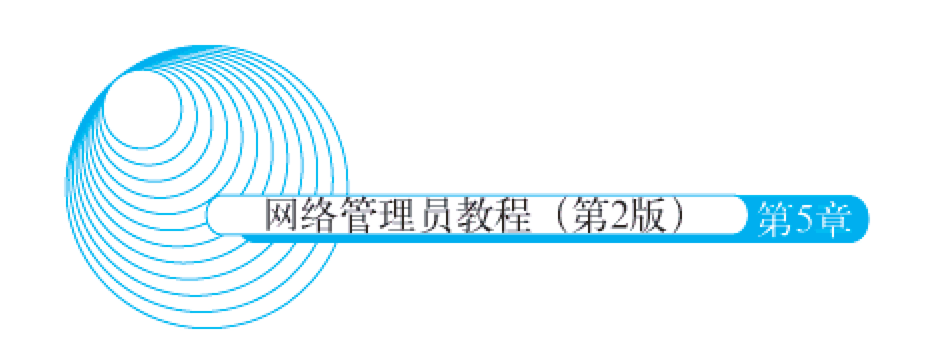
打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，选择相应的群组。单击菜单中的“操作”→“删除”，也可以右击选择快捷菜单中的“删除”项。出现提示时，请确认是否删除该群组。

删除群组会删除所有包含在其中的成员子网、主机、共享网络以及其他群组。如果想保留某个成员，请在删除群组之前将它移到将删除的群组之外。

5.5.7 选项的设置

在为客户机设置了基本的 TCP/IP 配置设置（如 IP 地址、子网掩码和默认网关）之后，大多数客户机同时还需要通过 DHCP 选项提供其他信息。在子网、主机、共享网络以及群组中没有指派的选项将自动套用其父系节点中指派的值。

（1）在 rfdhcp 配置工具主窗口左侧的控制台树中，展开想要配置其选项的服务器、子网、共



享网络或群组，选择“xxx 选项”（xxx 代表所选的节点名称）。单击菜单中的“操作”→“配置选项”，也可以选择右键快捷菜单中的“配置选项”菜单项。打开选项设置对话框，可以根据需要查看或修改对应节点的选项。

（2）在“可用选项”列表中，选中希望配置的对应选项，选中该选项前的复选框以激活窗口下面的“数据输入”框，输入该选项所需的必要信息。

（3）对于任何其他选项希望配置的选项，请重复以上的步骤，然后单击“确定”按钮。

5.5.8 rfdhcp 文件编辑器的使用

为了使用户能够全面地配置 DHCP 服务器支持的全部功能，rfdhcp 配置工具提供了一个文件编辑器。用户可以通过这个编辑器直接对 DHCP 配置文件进行手工修改。

配置工具也可以检查配置文件的语法错误。语法检查结果会显示在输出消息窗口中。

默认情况下，主窗口中不显示配置文件编辑区。在菜单中选择“查看”→“编辑器”，显示配置文件编辑窗口。

在编辑器窗口中对配置文件进行手工修改。单击工具栏上的“保存”按钮，储存文件，查看输出信息中的语法检查结果。如果出现语法错误，请根据提示进行修改。修改完成后，重复上面的步骤。

网络管理员在手工编辑配置文件时，请注意以下事项。

（1）在开始手工修改配置文件后，请不要在存储文件之前使用配置工具提供的其他配置功能，否则所做的修改将会被覆盖。

（2）配置文件修改并存储后，必须重新启动 DHCP 服务器才能使修改生效。

（3）输出信息中所显示的蓝色信息属于警告，红色信息属于错误。

（4）租约数据库文件不能用配置工具修改。修改租约文件可能会导致 DHCP 服务器掌握的租约信息不正确。因此在正常情况下，不应对租约文件做任何修改。

（5）可以使用如下的命令来指定配置文件和租约文件的路径：

```
rfdhcp - cf <configuration file> -lf <lease file>
```

（6）一般情况下，请不要指定自己的租约文件。租约信息不正确会影响 DHCP 服务器的正常工作。

5.6 代理服务器的配置

代理服务器是为了节约 IP 地址资源、降低因特网接入成本而采用的技术，它拥有 Internet 连接共享、提高访问速度以及节约贷款等诸多优点。

在局域网中实现代理服务器接入的时候，必须有一台专门的计算机作为代理服务器，为其他的计算机提供服务，代理服务器将网络分成了两段：一段连接因特网，接入的方法可以是PSTN、ISDN、ADSL、Cable Modem、LAN＋FTTX 等；另一段与局域网连接，通过集线器或交换机连接，如图 5-56 所示。

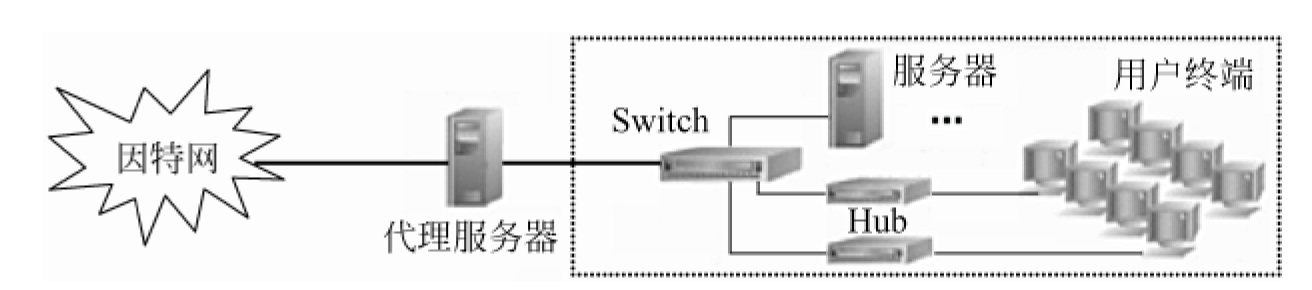


图 5-56　采用代理服务器接入因特网示意

通常代理服务器的实现有 Internet 连接共享（ICS，Internet Connection Share）、WinGate 以及 SyGate等多种方式，下面以 Windows 环境中的 WinGate 4.42 为例介绍代理服务器的实现。

5.6.1　WinGate 服务器端的安装

（1）双击 WinGate 的安装程序 Setup.exe。首先出现协议窗口，如图 5-57 所示。

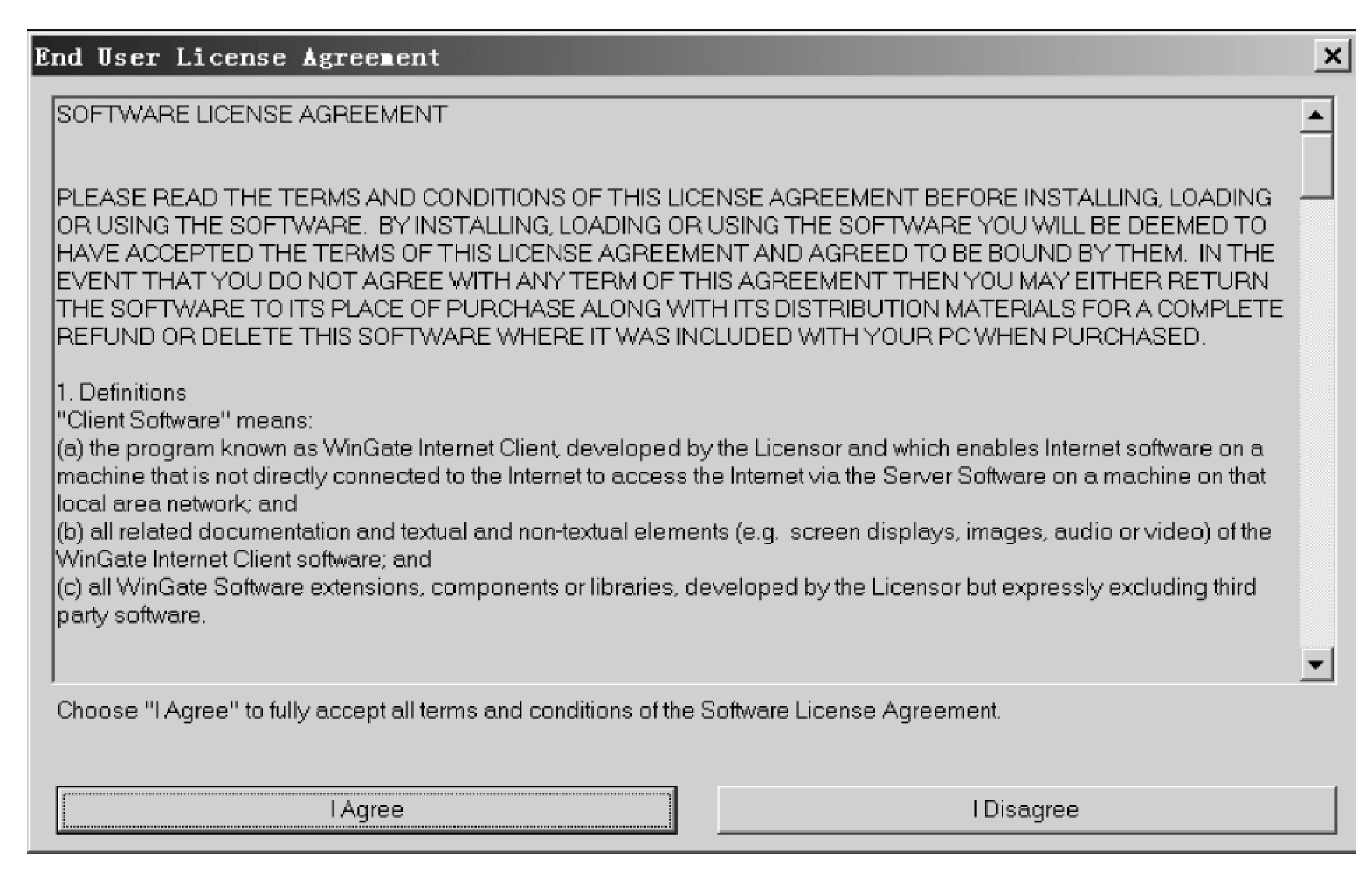
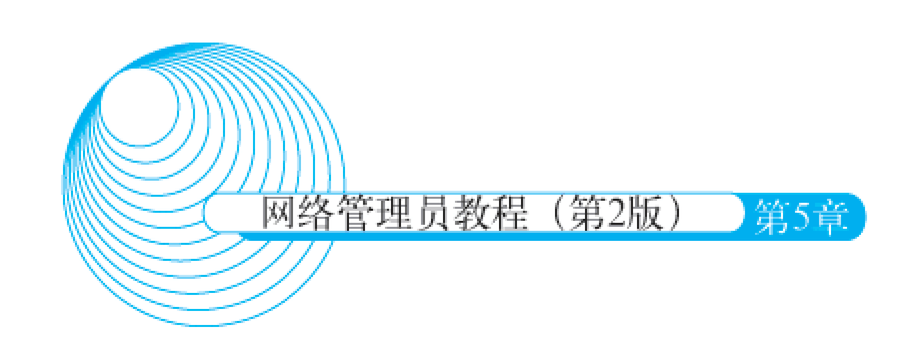


图 5-57　WinGate 协议窗口

（2）接受协议，单击 I Agree 按钮，系统出现安装类型选择窗口，询问是安装客户端还是安装



服务器端，选择 Configure this Computer as the WinGate Server 以确定安装服务器端，如图 5-58 所示。

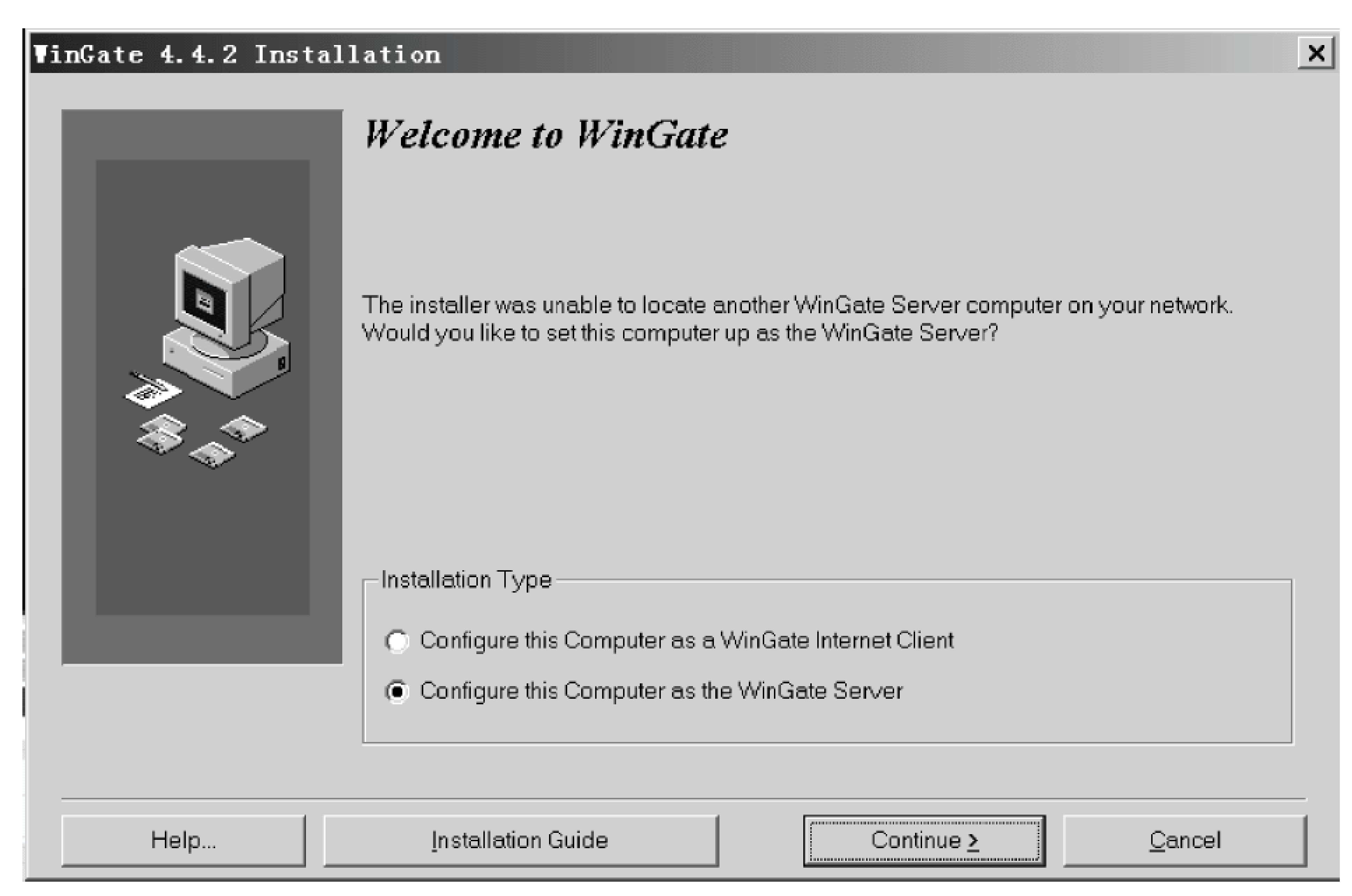


图 5-58　安装类型选择窗口

（3）单击 Continue 按钮，出现询问窗口，单击 Next 按钮确认安装。系统出现一系列选择窗口，询问是试用还是购买等，作出选择后，单击 Next 按钮。

（4）选择安装的路径，如图 5-59 所示。

（5）系统出现一系列选择窗口，询问安装的模式等，作出选择后，单击 Next 按钮，系统开始安装，并显示安装进度，如图 5-60 所示。安装结束时，单击 Finish 按钮完成安装。

5.6.2　WinGate 客户端的安装

（1）在图 5-58 所示窗口中选择 Configure this Computer as a WinGate Internet Client 以确定安装客户端。

（2）单击 Continue 按钮，出现询问窗口，如图 5-61 所示，单击 Next 按钮确认安装。

（3）系统进行安装，并显示安装进度。

（4）安装完成后系统出现一个提示窗口，如图 5-62 所示，单击 Finish 按钮。

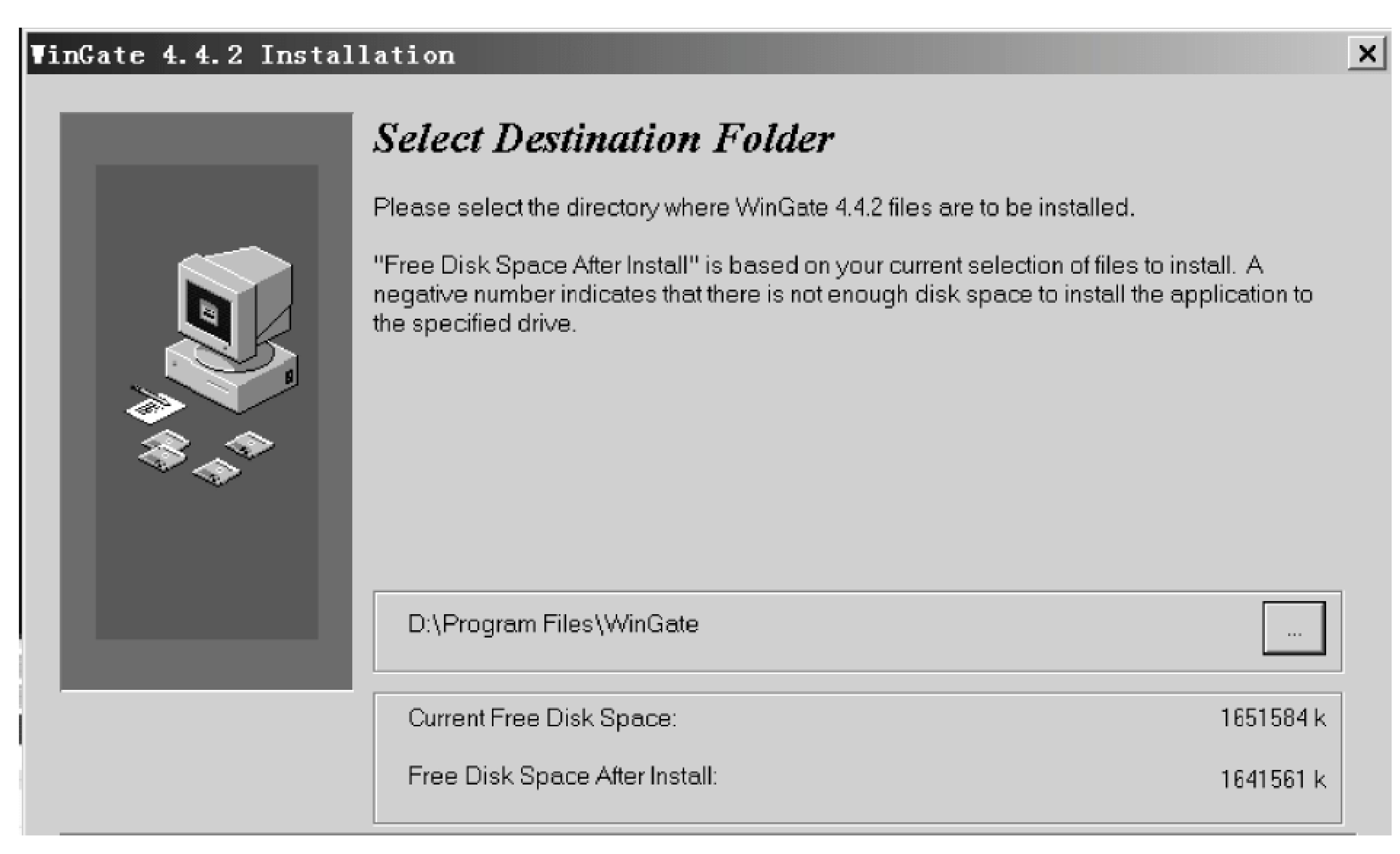


图 5-59 安装路径选择

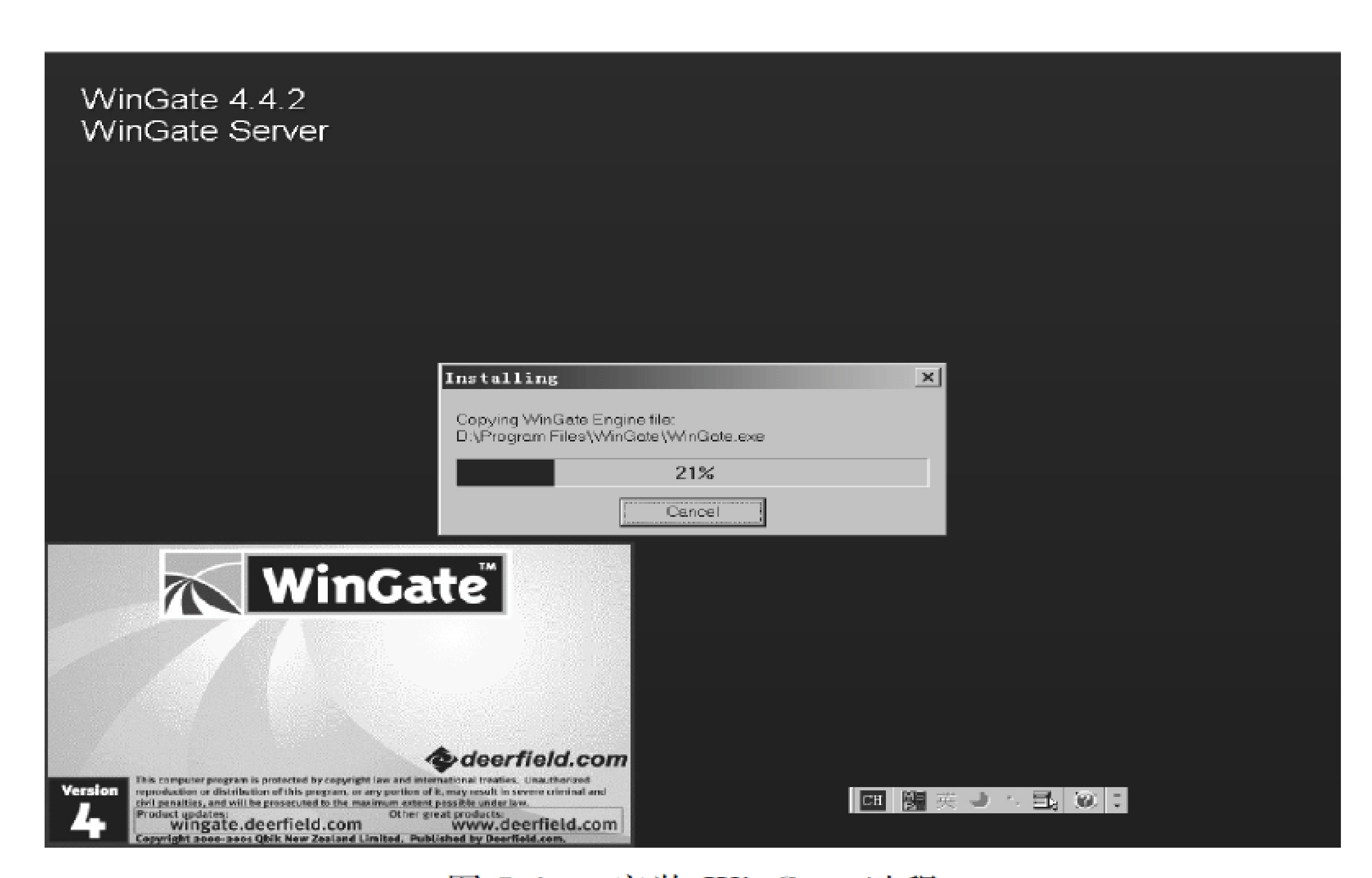


图 5-60 安装 WinGate 过程

5.6.3 WinGate 服务器端的基本设置

(1) WinGate 安装完毕后，默认状态下 WinGate 服务器和系统同时启动，也可以依次单击

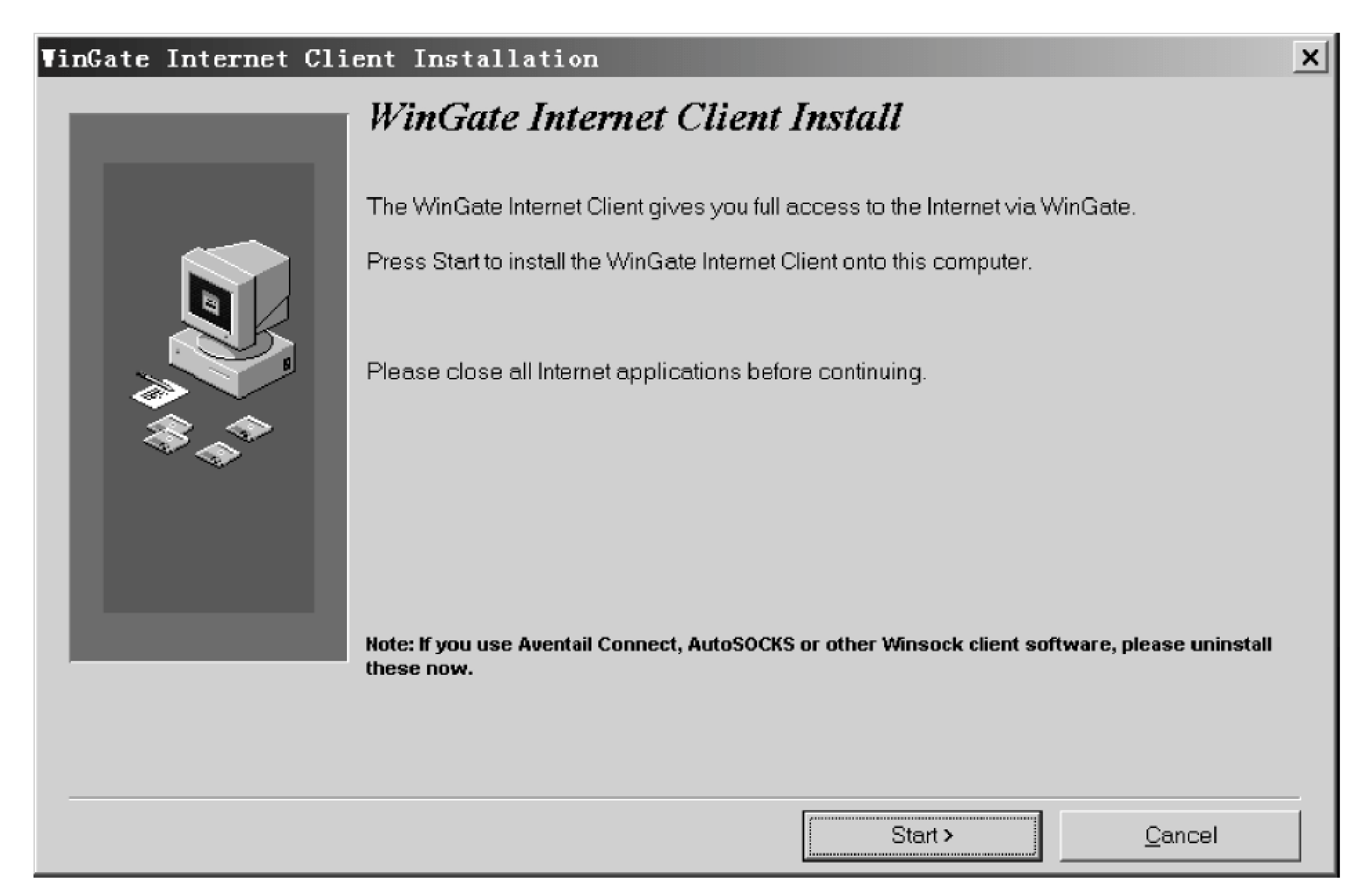


图 5-61　安装 WinGate 客户端



图 5-62　完成安装 WinGate 客户端

“开始”→“所有程序”→WinGate→Start WinGate Engine 选项，手工启动程序，启动后如图 5-63 所示。

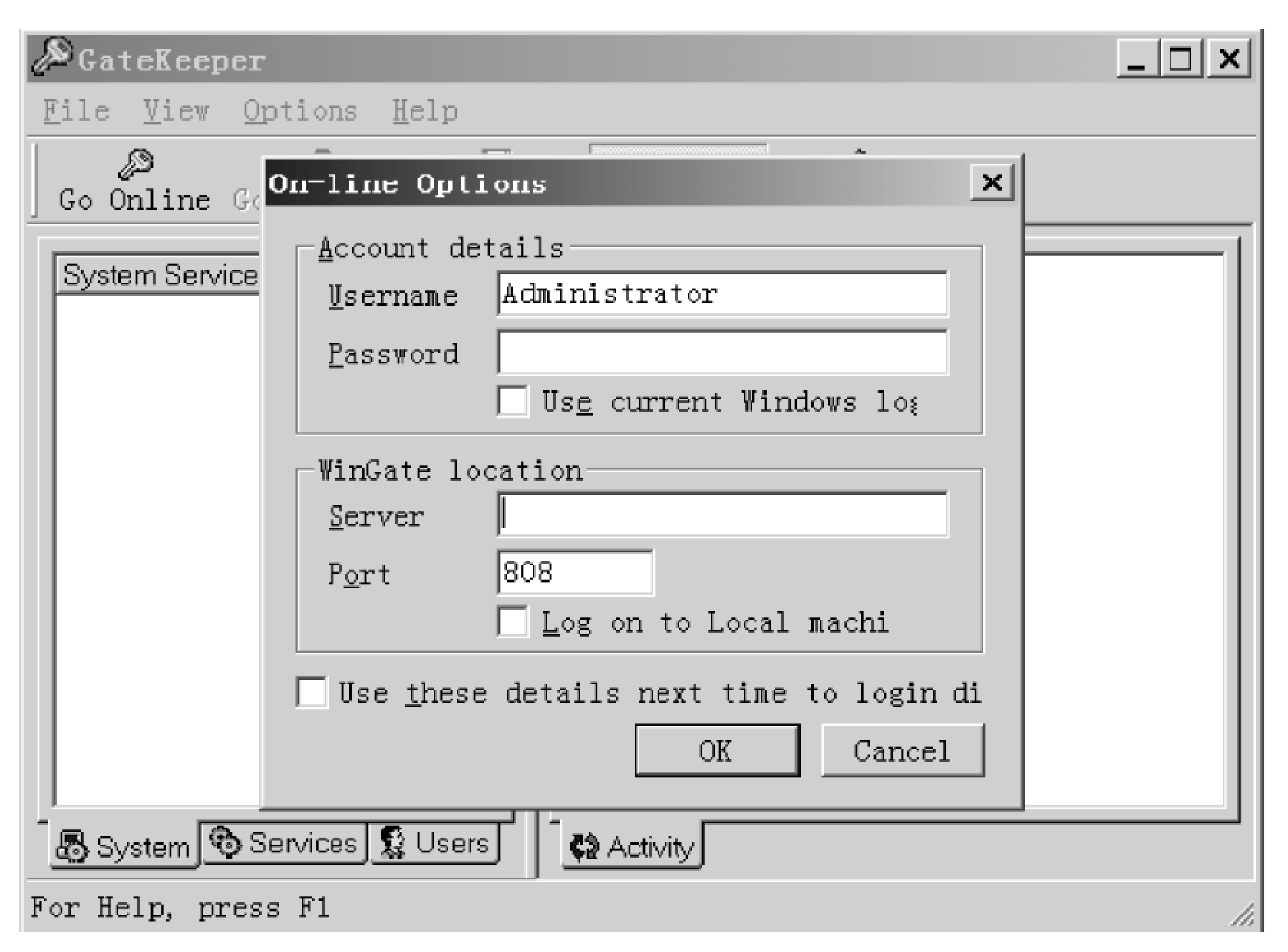


图 5-63　启动 WinGate

（2）WinGate 初次运行时的设置为：在 Username 文本框输入 administrator，密码文本框为空，选中 Log on to Local machi 复选框，登录本地服务器，如图 5-64 所示。

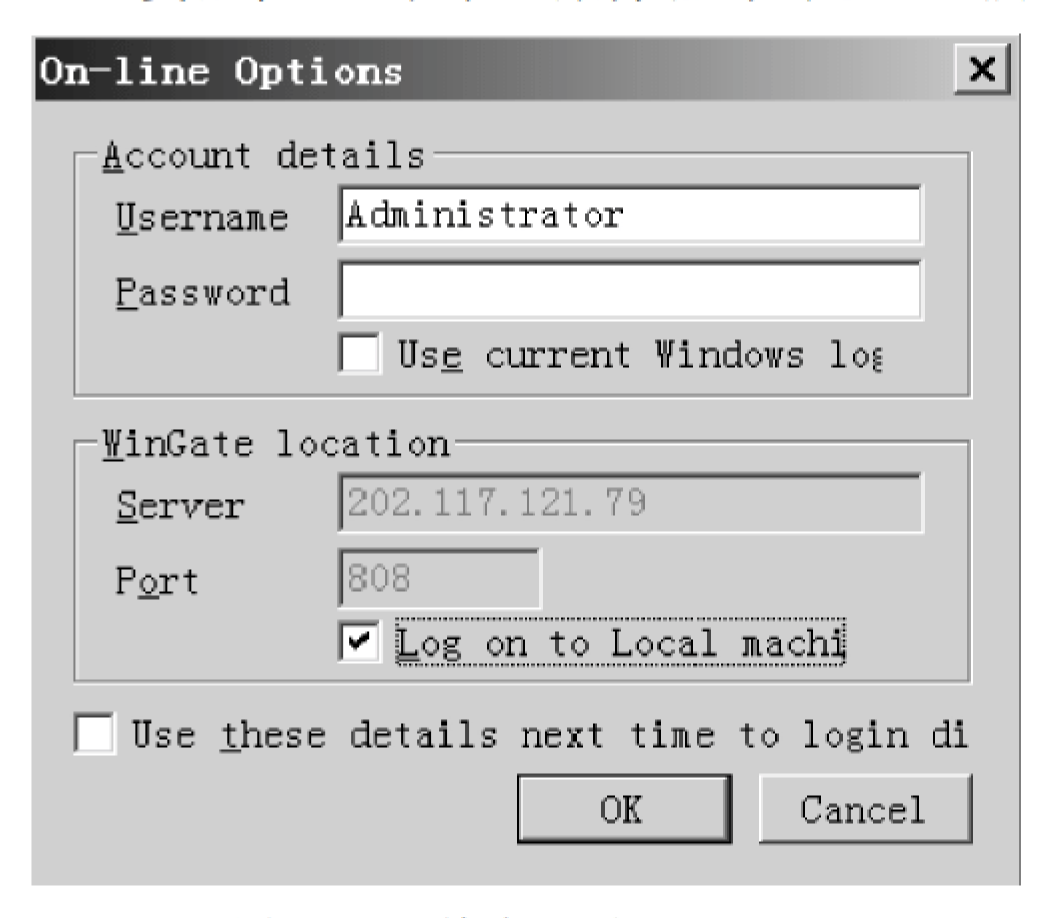
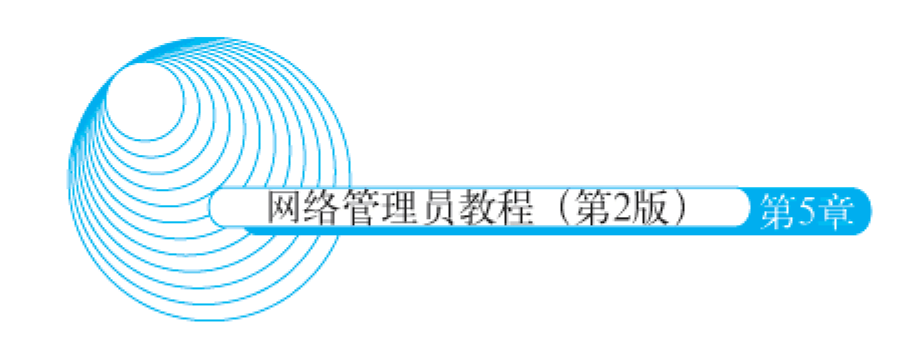


图 5-64　首次登录 WinGate



(3) 单击 OK 按钮，系统提示必须改变密码，否则无权进行后续操作，单击“确定”按钮，输入新密码，如图 5-65 所示。

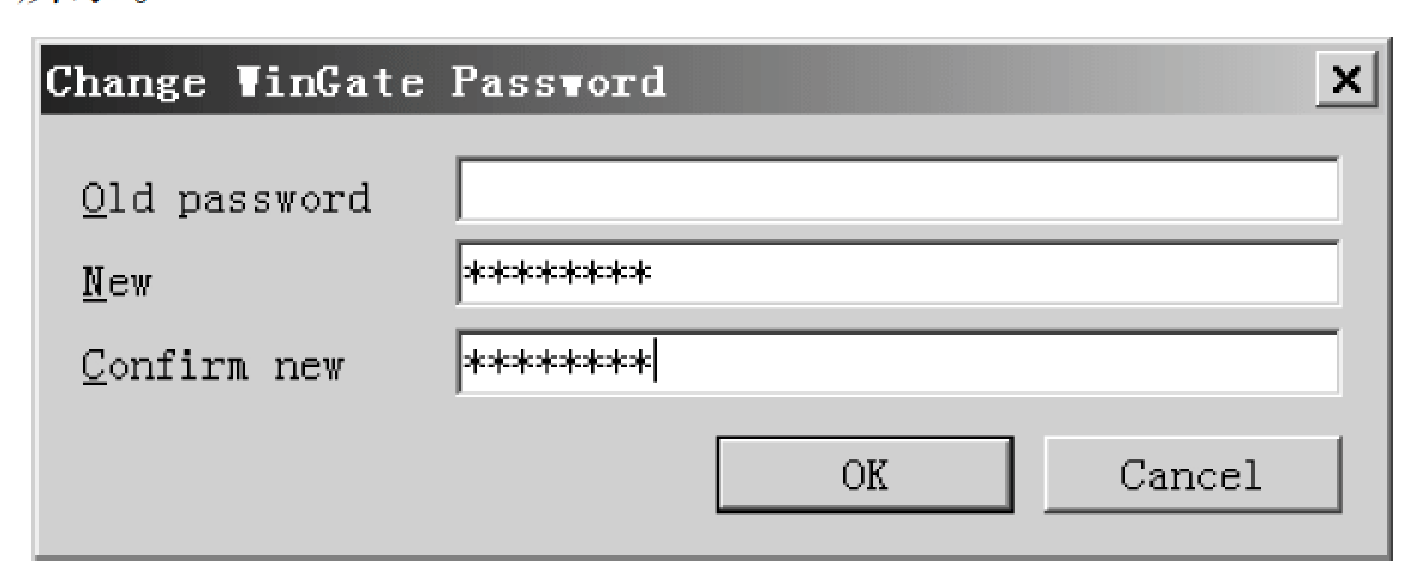


图 5-65　修改密码

(4) 单击 OK 按钮，系统自动加入服务、协议，以及用户组，分别如图 5-66、图 5-67 所示。

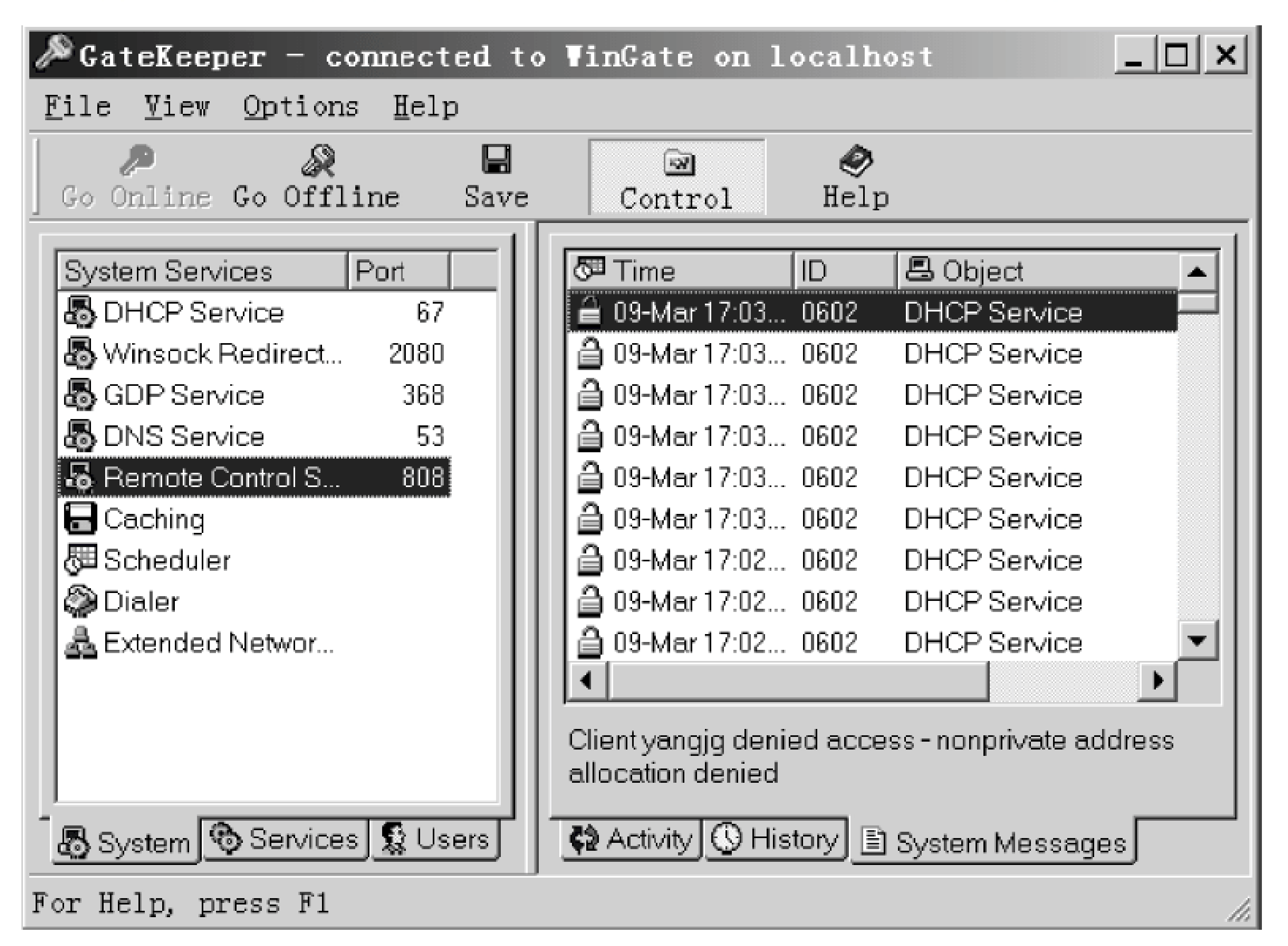


图 5-66　系统服务

(5) 在 System 选项卡中双击 Remote Control Service 进行远程控制服务配置，系统弹出其属性窗口，选择 Bindings 选项卡，双击 Available 栏目中的 IP 地址，将其选择到 Bound 栏目中，如图 5-68 所示。

(6) 单击 OK 按钮，在 System 选项卡中右击 Remote Control Service，然后单击 Start 启动服务，如图 5-69 所示。这样远程客户机就可以通过 Gatekeeper 来连接服务器了。

(7) 在 Service 选项卡中双击 WWW Proxy Server 进行远程访问代理，系统弹出其属性窗

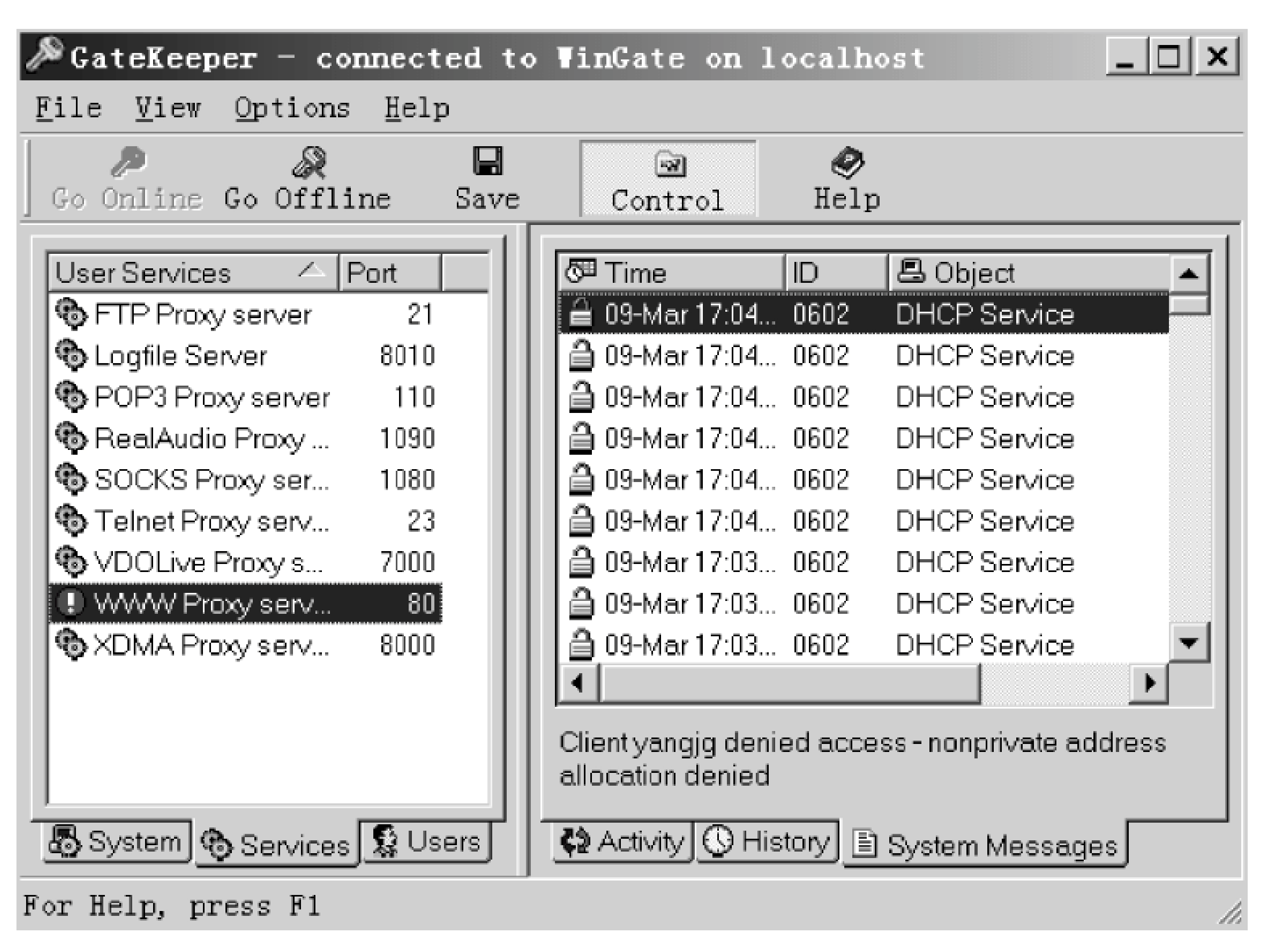


图 5-67 用户服务

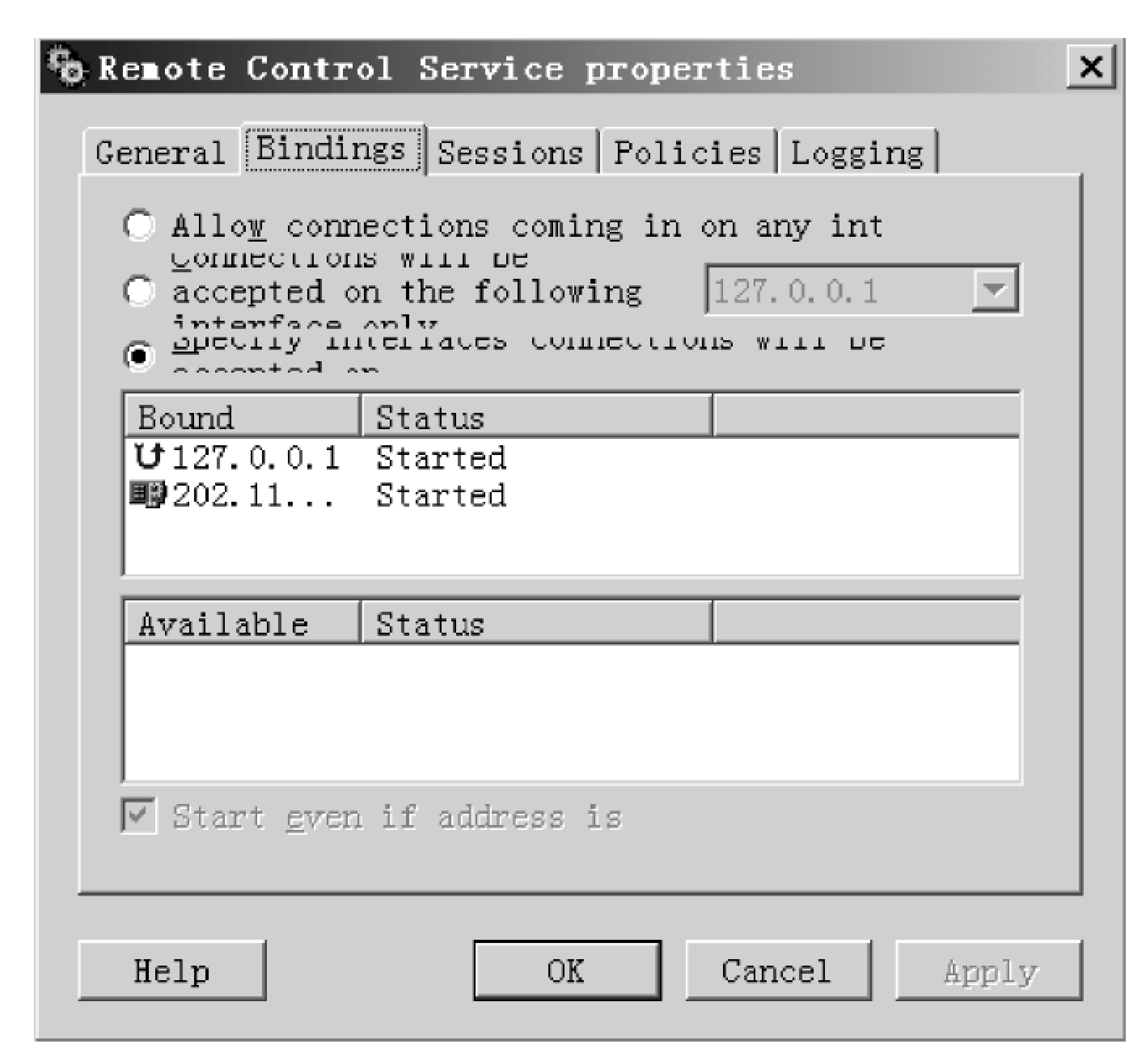


图 5-68 远程控制服务配置

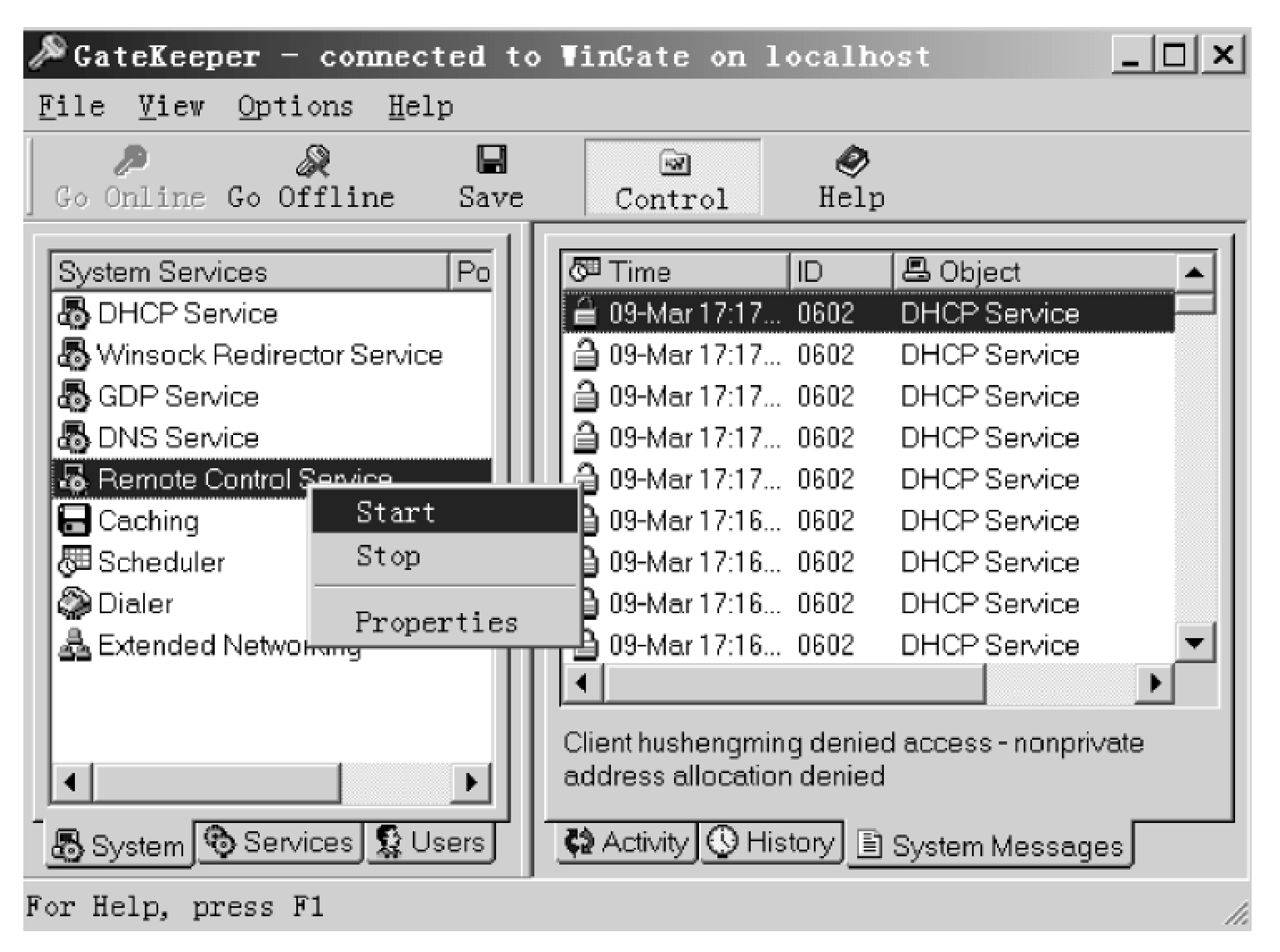


图 5-69　启动服务

口，选择 Connection 选项卡，选中 Through HTTP proxy with SSL tunneling 单选按钮，在 Server 文本框中输入代理服务器的 IP 地址，在 Port 文本框中输入端口号，如图 5-70 所示，单击 OK 按钮，设置好远程代理。

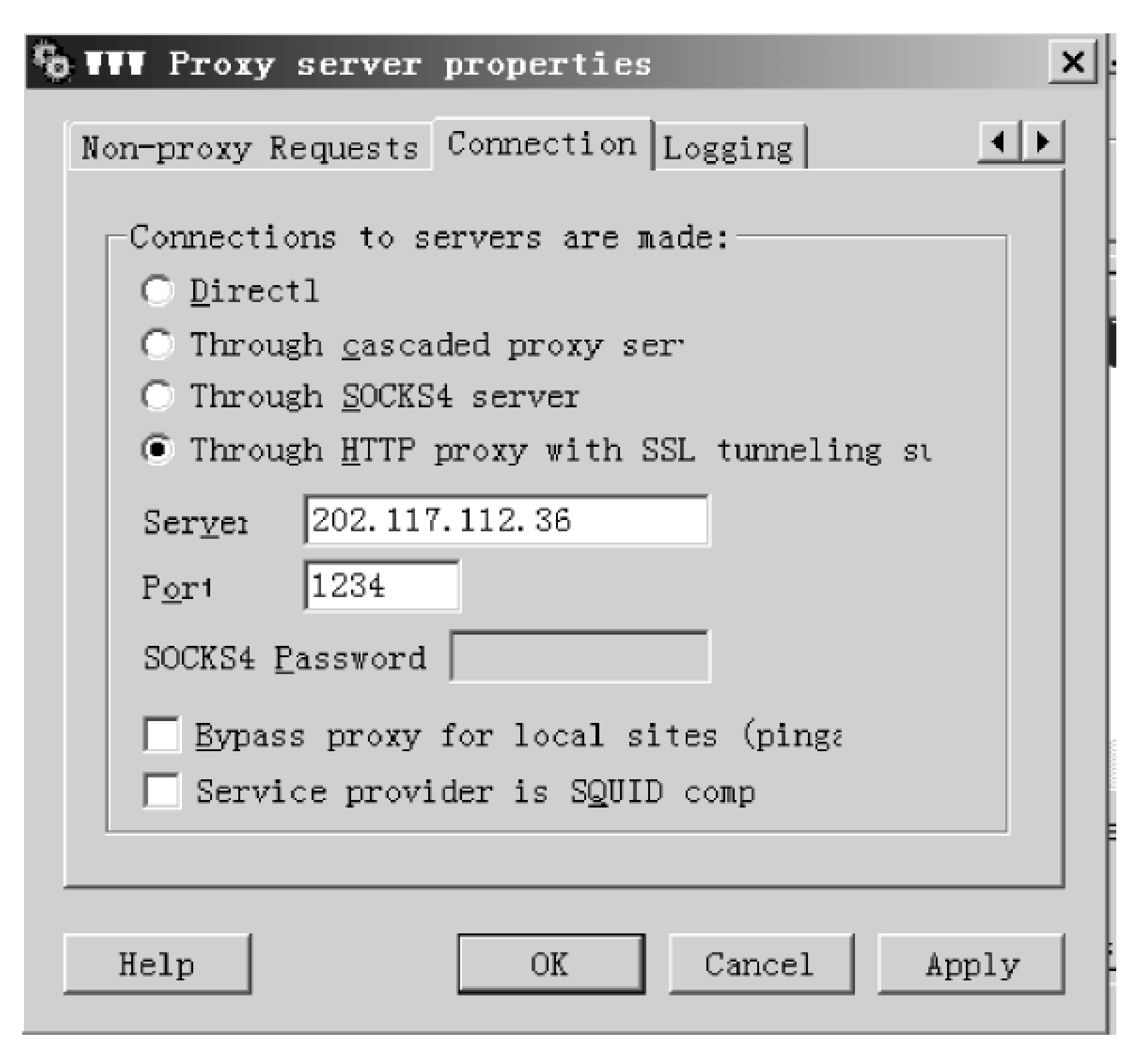


图 5-70　连接服务器

（8）在 Users 选项卡中右击 New User 或 New Group 进行用户和组的添加，如图 5-71 所示。

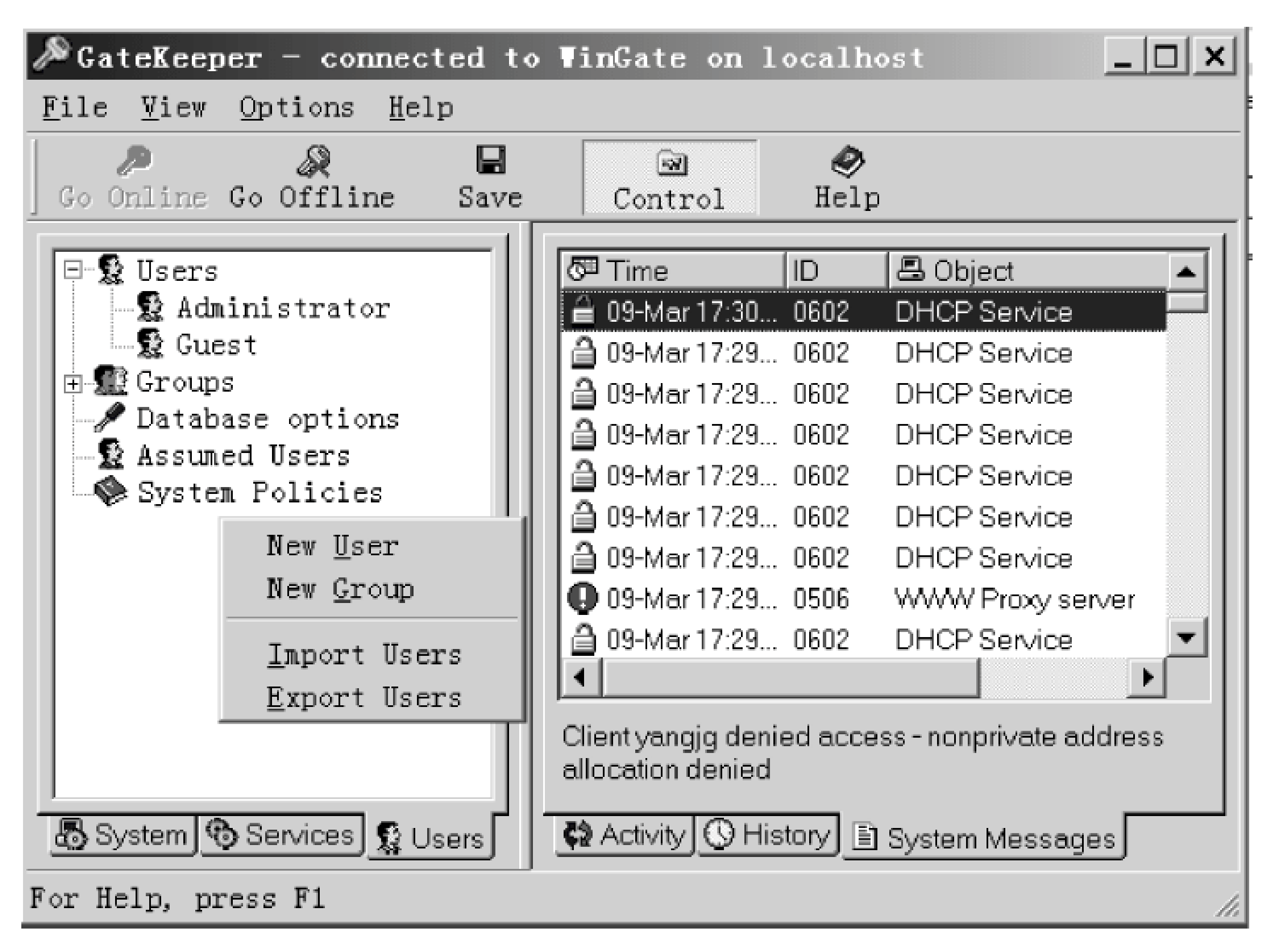
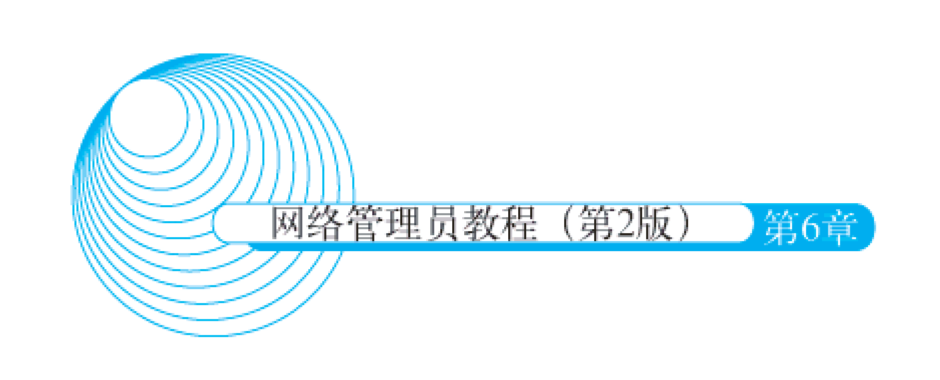


图 5-71　用户组的添加

这样就配置好 WinGate 服务器端，客户端启动 GateKeeper，输入用户名和密码就可以登录代理服务器。



第6章　Web网站建设

6.1　使用 HTML 制作网页

6.1.1　HTML 简介

目前因特网上绝大多数网页都是采用 HTML 文档格式存储的。HTML 是标准通用型标注语言(SGML，Standard Generalized Markup Language)的一个应用，是一种对文档进行格式化的标注语言。HTML 文档的扩展名为.html 或.htm。HTML 文档中包含大量的标记，这些标记是一些用来对网页内容进行格式化和布局的命令和指令，用于对页面中的信息进行格式化和布局，定义页面在浏览器中查看时的外观。例如，<B></B>标记表示文本使用粗字体。标记也用来指定超文本链接，这使得用户用鼠标单击该链接就能被引导到另一个页面。

1. HTML 元素

HTML 文档是标准的 ASCII 文档。从结构上讲，HTML 文档由元素(element)组成，组成 HTML 文档的元素有许多种，用于组织文档的内容和定义文档的显示格式。绝大多数元素是“容器”，即它有起始标记(start tag)和结束标记(end tag)。在起始标记和结束标记中间的部分是元素体。每一个元素都有名称和可选择的属性，元素的名称和属性都在起始标记内标明。例如以下 body 元素：

```
<body backgroud="back-ground.gif">
<h2> demo </h2>
This is my first html file. <p>
</body>
```

第 1 行是 body 元素的起始标记，它标明 body 元素从此开始。元素名称不分大小写。起始标记内的 background 是属性名，指明用什么方法来填充背景，其属性值为 back-ground.gif。一个元素可以有多个属性，属性及其属性值不分大小写。

第 2 行和第 3 行是 body 元素的元素体，最后一行是 body 元素的结束标记。

2. HTML 文档的组成

HTML 文档以<html>标记开始，以</html>结束，由文档头和文档体两部分构成。文档头由元素<head></head>标记，文档体由元素<body></body>标记。

文档头部分可以包含以下元素：

(1) 窗口标题。提供对 HTML 文档的简单描述，它出现在浏览器的标题栏。用户在收藏页面时显示的就是标题。

(2) 脚本语言。脚本是一组由浏览器解释执行的语句，能赋予页面更多的交互性。

(3) 样式定义。用来将页面样式与内容相分离的级联样式单。

(4) 元数据。提供了有关文档内容和主题的信息。

需要说明的是，这些元素书写的次序是无关紧要的，它只表明文档头有还是没有该属性。

文档体包含了可以在浏览器中显示的内容，它常常是 HTML 文档中最大的部分，文档体部分可以包含以下元素：

(1) 文本。文本内容可以使用适当的格式化元素放置在主体中，这些格式化元素将控制内容的显示方式。

(2) 图像。文档中的重要部分，使网页内容更加丰富。

(3) 链接。允许在网站中导航或到达其他的网站。链接通常放在页面主体中。

(4) 多媒体和特定的编程事件。通过放置在 HTML 文档主体中的代码来管理 Shockwave、SWF、Java Applet，甚至是在线视频。

3. HTML 文档的基本结构

以下代码表示了 HTML 文档的基本结构。

```
<html>
<head>
    <title> </title>
    …
</head>

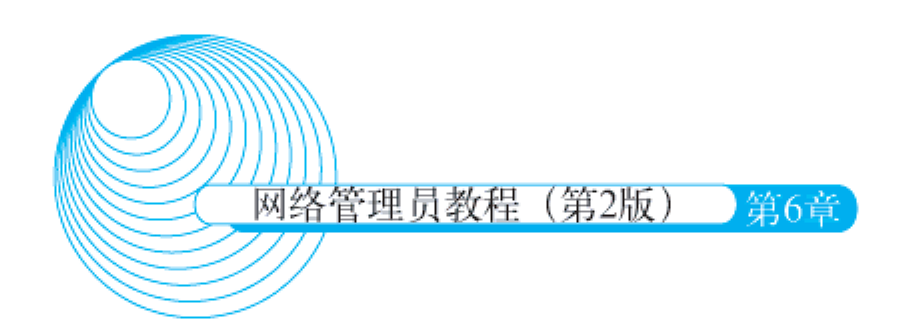
<body>
…
</body>

</html>
```

6.1.2 HTML 常用元素

1. 基本元素

1) 窗口标题(title)



title 元素是文档头中唯一一个必须出现的元素，格式为：

<title>窗口标题描述</title>

title 标明该 HTML 文档的标题，是对文档内容的概括，它出现在浏览器的标题栏。用户在收藏页面时显示的就是标题。标题元素是头元素中唯一必须出现的标记。title 的长度没有限制，一般情况下它的长度不应超过 64 个字符。

在头元素中还可以出现其他元素，如<isindex>、<meta>等。这些元素都不是必须的，而且也不常用。

2）页面标题

页面标题有 6 种，分别为 h_1、h2、…、h6，用于表示文章中的各种标题，标题号越小字体越大。一般情况下，浏览器对标题作如下解释。

（1）h1：黑体，特大字体，居中，上下各有两行空行。

（2）h2：黑体，大字体，上下各有一到两行空行。

（3）h3：黑体（斜体），大字体，左端微缩进，上下空行。

（4）h4：黑体，普通字体，比 h3 更多缩进，上边有一空行。

（5）h5：黑体（斜体），与 h4 相同缩进，上边有一空行。

（6）h6：黑体，与正文有相同缩进，上边有一空行。

hn 还可以有对齐属性 align，属性值可以为 left（标题居左）、center（标题居中）或 right（标题居右）。例如：

<h2 align=center>Chapter 2 </h2>

3）字体

（1）字体大小：HTML 有 7 种字号，1 号最小，7 号最大，默认字号为 3。可以用<basefontsize=字号>设置默认字号。

设置文本字号有两种办法：一种是设置绝对字号，<font size=字号>；另一种是设置文本的相对字号，<font size=±n>。用第二种方法时“+”号表示字体变大，“－”号表示字体变小。

（2）字体风格：字体风格分为物理风格和逻辑风格。物理风格直接指定字体，字体有黑体<b>、斜体<i>、下划线<u>、打字机体<tt>。逻辑风格指定文本的作用，字体有强调<em>、特别强调<strong>、源代码<code>、例子<samp>、键盘输入<kbd>、变量<var>、定义<dfn>、引用<cite>、较小<small>、较大<big>、上标<sup>、下标<sup>等。

（3）字体颜色：字体的颜色用<font color=#>指定。#可以是 6 位十六进制数，分别指定红、绿、蓝的值，也可以是 black、teal 、olive、red、blue、maroon、navy、gray、lime、white、green、purple、sliver、yellow、aqua 之一。

(4) 闪烁：<blink>文本</blink>使文本闪烁，闪烁频率为1秒钟一次。

4）横线

横线一般用于分隔同一文体的不同部分。在窗口中划一条横线非常简单，只要写一个<hr>即可。

5）分行和禁止分行

表示在此处分行。禁止分行<nobr>…</nobr>通知浏览器：其中的内容在一行内显示，若一行内显示不了，则超出部分被裁剪掉。

6）分段

HTML浏览器是基于窗口的，用户可以随时改变显示区的大小，所以HTML将多个空格以及回车等效为一个空格，这是和绝大多数字处理器不同的。HTML的分段完全依赖于分段元素<p>。比如下面两段源文档有相同的输出。

```
<h2>This is a level Two Heading </h2>
paragraphy one <p>paragraph two <p>

<h2>This Is a Level Two Heading</h2>
paragraph one <p>
paragraph Two <p>
```

<p>也可以有多种属性，比较常用的属性是align。例如：

```
<p align=center>This is a centered paragraph </p>
```

当HTML文档中有图形，图形可能占据了窗口的一端，图形的周围可能还有较大的空白区。这时，不带clear属性的<p>可能会使文章的内容显示在该空白区内。为确保下一段内容显示在图形的下方，可使用clear属性。clear属性值可以为left（下一段显示在左边界处空白的区域）、right（下一段显示在右边界处空白的区域）或all（下一段的左右两边都不许有别的内容）。

7）转义字符与特殊字符

HTML使用的字符集是ISO &859 Larin-1字符集，该字符集中有许多标准键盘上无法输入的字符。对这些特殊字符只能使用转义序列。例如HTML中<、>和&有特殊含义（前两个字符用于链接签，&用于转义）不能直接使用。使用这3个字符时，应使用它们的转义序列。

& 的转义序列为 & amps 或 & #38，<的转义序列为 &lt 或 & #60，>的转义序列为 &gt 或 & #62。前者为字符转义序列，后者为数字转义序列。例如：& Lt;font &Lgt;显示为<font>若直接写为<font>则被认为是一个链接签。

另一个需要转义的字符是引号，它的转义序列为“"”或“& #34;”。例如<img src=″image.gif″ alt=″A &quol; real " example″>。

需要说明的是：

（1）转义序列各字符间不能有空格；
（2）转义序列必须以“；”结束；
（3）单独的 & 不被认为是转义开始。
8）背景和文本颜色
窗口背景可以用下列方法指定：

```
<body background="image-URL">
<body bgcolor=# text=# link=# alink=# vlink=#>
```

前者指定填充背景的图像，如果图像的大小小于窗口大小，则把背景图像重复，直到填满窗口区域。后者指定的是十六进制的红、绿、蓝分量。其中：

（1）bgcolor 表示背景颜色；
（2）text 表示文本颜色；
（3）link 表示链接指针颜色；
（4）alinik 表示活动的链接指针颜色；
（5）vlinik 表示已访问过的链接指针颜色。

例如：<body bgcolor=FF0000>红背景色。

注意：*此时体元素必须写完整，即用</body>结束。*

9）图像（image）

图像使页面更加漂亮，但是图像会导致网络通信量急剧增大，使访问时间延长。所以在主页（Homhepage）中，不宜采用很大的图像。如果确实需要一些大图像，最好在主页中用一个缩小的图像指向原图，并标明该图的大小。

（1）图像的基本格式：<img src="image-URL">或<img src="image-URL" alt="text">。其中 image-URL 是图像文件的 URL，alt 属性告诉不支持图像的浏览器用 text 代替该图。

（2）图像与文本的对齐方式：图像在窗口中会占据一块空间，在图像的左右可能会有空白，不加说明时，浏览器将随后的文本显示在这些空白中，显示的位置由 align 属性指定。当 align=left 或 align=right 时，图像是一个浮动图像。例如：若 align=left 则图像必须挨着左边框，它把原来占据该块空白的文本“挤走”，或挤到它右边，或挤到它上下。文本与图像的间距用 vspace=# 和 hspace=# 指定，# 是整数，单位是像素。其中前者指定纵向间距，后者指定横向间距。

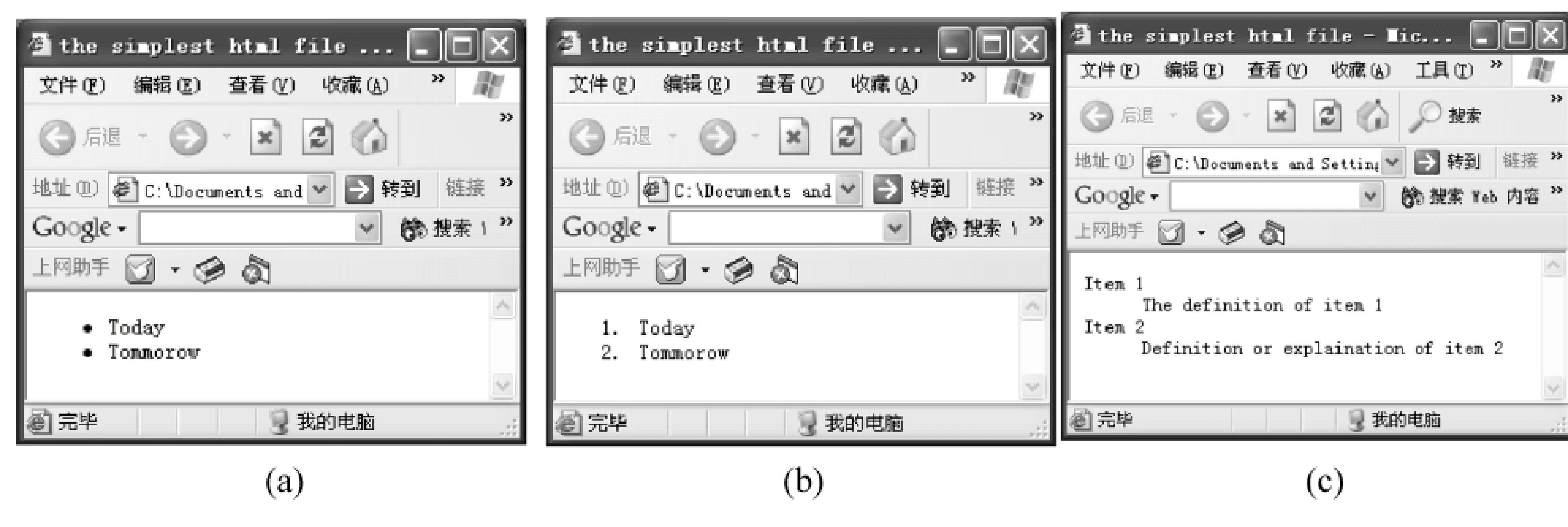
10）列表（list）

列表用于列举事实，常用的列表有 3 种格式，即无序列表（unordered list）、有序列表（ordered list）和自定义列表（definition list）。各种列表的输出结果如图 6-1 所示。

（1）无序列表：以
开始，每一个列表条目用
引导，最后是。

注意：*列表条目不需要结尾链接签。*

输出时每一列表条目缩进，并且以黑点标示。例如：



(a) (b) (c)

图 6-1 列表输出效果

```
<ul>
<li>Today
<li>Tomorrow
</ul>
```

（2）有序列表：与无序列表相比，只是在输出时列表条目用数字标示，以
开始，以
结束。下面是一个例子：

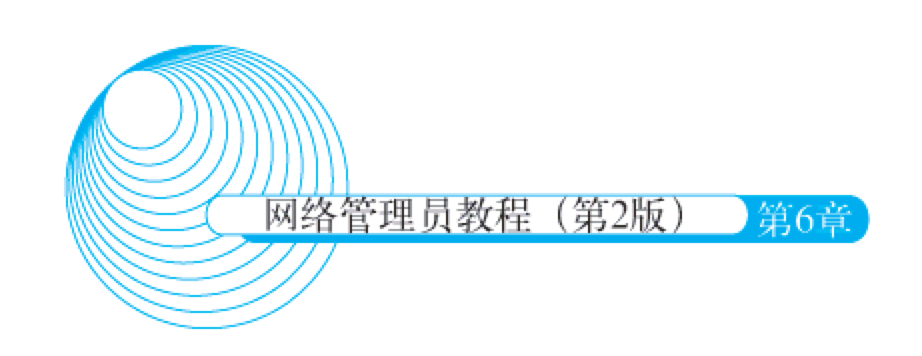
```
<ol>
<li>Today
<li>Tomorrow
</ol>
```

（3）自定义列表：用于对列表条目进行简短说明的场合，以<dl>开始，列表条目用<dt>引导，它的说明用<dd>引导。例如：

```
<dl>
<dt>Item 1
<dd>The definition of item 1
<dt>Item 2
<dd>Definition or explanation of item 2
</dl>
```

2. 超文本链接

超文本链接是 HTML 最吸引人们的优点之一。一个超文本链接由两部分组成：一是被指向的目标。它可以是同一文档的另一部分，也可以是远程主机的一个文档，还可以是动画或音乐；另一部分是指向目标的链接。使用超文本链接可以使顺序存放的文档具有一定程度上的随



机访问能力，这更加符合人类的思维方式。人的思维是跳跃的、交叉的，而每一个链接正好代表了作者或者读者的思维跳跃。

1）统一资源定位器(URL，Uniform Resource Locator)

统一资源定位器用于指定访问该文档的方法。一个URL的构成为：

protocol:// machine.name[:port]/directory/filename

其中：

(1) protocol是访问该资源所采用的协议，即访问该资源的方法，它可以是http(超文本传输协议，指向HTML资源)、ftp(文件传输协议，指向文件资源)、news(指向网络新闻资源)等。

(2) machine.name用于存放该资源主机的IP地址，通常以字符形式出现。

(3) port用于存放该资源主机中相关服务器所使用的端口号。一般情况下端口号不需要指定。只有当服务器所使用的端口号不是默认的端口号时才指定。

(4) directory和filename是该资源的路径和文件名。

2）指向一个目标<a>

在HTML文档中用链接指向一个目标。其基本格式为：

字符串

href属性中的统一资源定位器(URL)是被指向的目标，随后的字符串在HTML文档中充当指针的角色，其字体一般显示为带下划线的蓝色。当读者用鼠标单击这个字符串时，浏览器就会将URL处的资源显示在屏幕上。

3）标记一个目标

前面提到的链接可以在整个因特网上方便地链接。但如果编写了一个很长的HTML文档，往往需要在同一文档的不同部分之间也建立起链接，使用户方便地在上下方之间跳转。

标识一个目标的方法为：

text

name属性将放置该标记的地方标记为name，name是一个全文唯一的标记串，text部分可有可无。这样，就把放置标记的地方做了一个叫做name的标记。做好标记后，可以用下列方法来指向它。

text

URL是放置标记的HTML文档的URL，name是标记名。对于同一个文档，可以写为：

text

这时就可以单击text跳转到标记名为name的部分了。

4）图像链接

图像也可以建立链接。格式为：

```
<a href="URL"><img src="URL"></a>
```

可以看出，上例中用<img src="URL">取代了链接中 text 的位置。

下面是一个简单的图像链接。

```
<a href="www.ihep.ac.cn">China home page<img src="flag.gif"></a>
```

5）图像地图

上面介绍的图像链接每幅图只能指向一个地点，而图像地图可以把图像分成多个区域，每个区域指向不同的地点。可以用图像地图编出很漂亮的 HTML 文档。

图像地图不仅需要在 HTML 文档中说明，还需要一个后缀为.map 的文件，用来说明图像分区及其指向的 URL 的信息。在.map 文件中说明分区信息的格式如下：

（1）rect 指定一个矩形区域，该区域的位置由左上角坐标和右下角坐标说明。

（2）poly 指定一个多边形区域，该区域的位置由各顶点坐标说明。

（3）circle 指定一个圆形区域，区域位置由垂直通过圆心的直径与该圆的交点坐标说明。

（4）default 指定图像地图其他部分的 URL。坐标的写法为：x，y，各点坐标之间用空格分开。

图像地图需要一个特殊的处理程序 imagemap。imagemap 放在/cgi-bin 中。在 HTML 文档中引用图像地图的格式为：

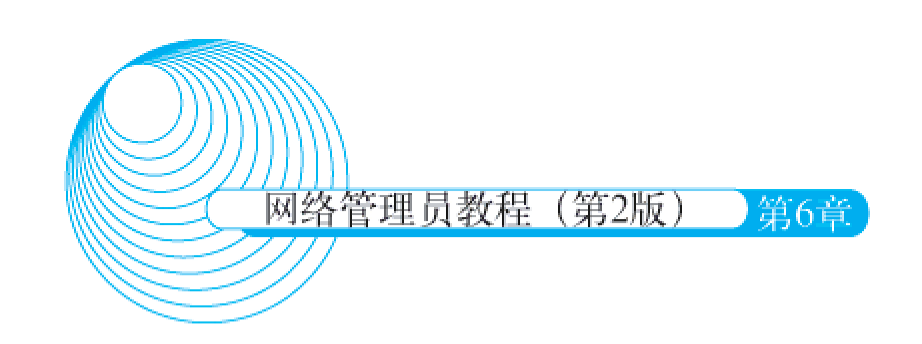
```
<a href="/cgi-bin/imagemap/mymap.map">
<img src="mymap.gif" ismap></a>
```

可以看出这是一个包含图像元素的链接元素。图像元素指明用于图像地图的图像的 URL，并用 Ismap 属性说明。需要说明的是链接中的 href 属性，它由两部分组成：第一部分是/cgi-bin/imagemap，它指出用哪个程序来处理图像地图，必须原样写入；第二部分才是图形地图的说明文件 mymap.map。在 netscape 扩展中，图像地图可以用一种比较简化的方式来表示，这就是客户端图像地图。用户端地图可以将图像地图的说明文件写在 HTML 文档中，而且不需要另外的程序来处理。这就使 HTML 作者可以用同类别的元素相一致的写法来写图像地图。客户端图像地图还有一个优点，当鼠标指向图像地图的不同区域时，浏览器能显示出各个区域所指向的 URL。

用户端图像地图的格式为：

```
<img src="URL" usemap="#mymap">
```

其中，src="URL" 指定用作图像地图的图像，usemap 属性指明这是客户端图像地图，"#mymap"



是图像文件说明部分的标记名，浏览器寻找名字为 mymap 的<map>元素并从中得到图像地图的分区信息。

客户端图像地图的分区信息用<map name=mapname>元素说明，name 属性命名<map>元素。

图像地图的各个区域用<area shape="形状" coords="坐标" href="URL">说明，形状可以是：rect 表示矩形，用左上角、右下角的坐标表示，各个坐标值之间用逗号分开；poly 表示多边形，用各顶点的坐标值表示；circle 表示圆形，用圆心及半径表示，前两个参数分别为圆心的横、纵坐标，第 3 个参数为半径。

href="URL"表示该区域指向资源的 URL，也可以是 nohref，表示在该区域鼠标点取无效。

客户端图像地图各个区域可以重叠，重叠区以先说明的条目为准，下面是一个例子：

```
<img src="mapimg.gif" usemap="#Face>
<map name="Face">
<! Text BOTTON> 此行是注释
<area shape="rect"
href="page.html"
coords="140,20,280,60">
<! Triangle BOTTON>
<area shape="poly"
href="image.html"
coords="100,100,180,80,200,140">
<! FACE>
<area shape="circle"
href="nes.html"
coords="80,100,60">
</map>
```

3. 表格(Table)

1) 表格的基本形式

一个表由<table>开始，</table>结束，表的内容由<tr>、<th>和<td>定义。<tr>说明表的一个行，表有多少行就有多少个<tr>。<th>说明表的列数和相应栏目的名称，有多少个列就有多少个<th>。<td>则填充由<tr>和<th>组成的表格。

2) 有通栏的表

有横向通栏的表用<th colspan=#>属性说明。colspan 表示横向栏距，# 代表通栏占据的网格数，它是一个小于表的横向网格数的整数。有纵向通栏的表用 rowspan=# 属性说明。

rowspan 表示纵向栏距，# 表示通栏占据的网格数，应小于纵向网络数。需要说明的是有纵向通栏的表，每一行必须用</tr>明确给出横向栏目结束，这是和表的基本形式不同的。

3）表的大小、边框宽度和表格间距

表的大小用 width=# 和 height=# 属性说明。前者为表宽，后者为表高，# 是以像素为单位的整数。

边框宽度由 border=# 说明，# 为宽度值，单位是像素。

表格间距即划分表格的线的粗细，用 cellspacing=# 表示，# 的单位是像素。

4）表中文本的输出

文本与表框的距离用 cellpadding=# 说明。表格的宽度大于其中的文本宽度时，文本在其中的输出位置用 align=# 说明。# 是 left、center 和 right 三者之一，分别表示左对齐，居中和右对齐，align 属性可修饰<tr>、<th>和<td>链接签。

表格的高度大于其中文本的高度时，可以用 valign=# 说明文本在其中的位置。# 是 top、middle、bottom、baseline 四者之一。分别表示上对齐，文本中线与表格中线对齐，下对齐，文本基线与表格中线对齐。特别注意的是 baseline 对齐方式，它使得文本出现在网格的上方而不是想象中的下半部。同样，valign 可以修饰<tr>、<th>、<td>中的任何一个。

5）浮动表格

所谓浮动表格是指表与文档中内容对齐时，若在现在位置上不能满足其对齐方式，表格可上下移动，即“挤开”一些内容，直到满足其对齐要求。一般由 align=left 或 right 指定。

6）表格颜色

表格的颜色用 bgcolor=# 指定。

是 16 进制的 6 位数，格式为 rrggbb，分别表示红、绿、蓝 3 种颜色的分量。或者是 16 种已定义好的颜色名称。

4. 框架(Frame)

框架将浏览器的窗口分成多个区域，每个区域可以单独显示一个 HTML 文档，各个区域也可相关联地显示某一个内容。例如：可以将索引放在一个区域，文档内容显示在另一个区域。框架的基本结构如下：

```
<html>
<head>
<title>…</title>
</head>
<noframes>…</noframes>
<frameset>
<frame src="URL">
```

```
</frameset>
</html>
```

可以在框架中安排行或列并确定这些行或列的 HTML 页面，这是通过以下标记完成的。

（1）<frameset>标记。该标记定义了结构，它的基本参数定义了行或列，<frameset>在框架 HTML 页面中的概念相当于<body>，在简单的框架中不应出现 body 标记。

（2）<frame>标记。该标记在框架中排列单独框架。包括通过 src="x"来填充框架中所需的 HTML 文档的位置。

（3）<noframes>标记。当浏览器不支持框架时就显示这个标记的内容。

在框架中可以使用如下属性：

（1）cols="x"。这个属性可以创建多个列。框架页面的每一列都给出了一个 x 值，这样就可以创建动态或相对大小的框架。每列的属性值之间用逗号分开。例如，一个有 3 列框架的 cols 属性是 cols="200，150，*"，表示第 1 列宽 200 像素，第 2 列宽 150 像素，第 3 列由剩余像素组成。

（2）rows="x"。使用列属性的方式来创建行。

（3）border="x"。这个值按像素设置宽度。

（4）frameborder="x"。IE 浏览器用它来控制边界的宽度。

（5）framespacing="x"。这个属性最初由 IE 浏览器使用，用来控制边界宽度。

框架标记使用以下属性：

（1）frameborder="x"。使用这个属性来控制单个框架周围的边界。

（2）marginheight="x"。根据像素来控制框架边界的高度。

（3）marginwidth="x"。按像素来控制框架边界的宽度。

（4）name="x"。这个属性允许设计者命名一个单独的框架。命名框架可以作为其他 HTML 页面中链接的目标。名称必须以标准的字母或数字开头。

（5）noresize。这个属性固定了框架的位置且不允许用户改变框架大小，该属性不需要属性值。

（6）scrolling="x"。通过选择 yes、no 或 auto，可以控制滚动条的外观。yes 为在框架中自动放置滚动条，值为 no 则不出现滚动条，值为 auto 则在需要时自动放置一个滚动条。

（7）src="x"。x 的值由想要放置在框架中的 HTML 页面的相对或绝对 URL 来代替。

6.1.3 HTML 应用实例

本小节将介绍一个实例，并对其内容进行分析。

```
<html>
```

```
<head>
<meta http-equiv="Content-Type" content="text/html; Charest=gb2312">
<title>意境</title>
</head>
<body>
<table border="0" width="100%" cellpadding="0">
<tr>
<td width="100%"><p align="center"><font face="隶书" size="6" color="#FF00FF">
<strong>欢迎进入本站</strong></font></td>
</tr>
</table>
<table border="0" width="100%" cellspacing="0" cellpadding="0">
<tr>
<td width="100%"><table border="0" width="100%" cellspacing="0" cellpadding="0">
<tr>
<td width="10%" valign="top" align="center"></td>
<td width="80%" valign="top"><table border="0" width="100%" cellspacing="0" cellpadding
="0">
<tr>
<td width="17%"></td>
<td width="17%">
<a href="http://202.103.176.80/g/speaker/cool.htm">
<img src="http://202.103.176.80/g/speaker/huaren/mypic1.gif" alt="共享程序网站入口" border
="0" width="180" height="90"></a></td>
<td width="17%"></td>
</tr>
<tr>
<td width="17%"></td>
<td width="17%"></td>
<td width="17%"></td>
</tr>
<tr>
<td width="17%">
<img src="http://202.103.176.80/g/speaker/huaren/mypic2.gif"
alt="个人作品网站入口" width="180" height="90"></td>
<td width="17%"></td>
<td width="17%"><a href="http://202.103.176.80/g/speaker/dault.htm">
```

```
<img src="http://202.103.176.80/g/speaker/huaren/mypic4.gif" alt="主页入口" border=
"0"></a></td>
</tr>
<tr>
<td width="17%"></td>
<td width="17%"> <p> </td>
<td width="17%"></td>
</tr>
<tr>
<td width="17%"></td>
<td width="17%">
<img src="http://202.103.176.80/g/speaker/huaren/mypic3.gif" alt="推荐网站入口">
</td>
<td width="17%"></td>
</tr>
</table>
</td>
<td width="10%" valign="top" align="center"></td>
</tr>
<tr>
<td width="10%"></td>
<td width="80%"></td>
<td width="10%"></td>
</tr>
</table>
</td>
</tr>
</table>
<p> </p>
<table border="0" width="100%" cellpadding="0">
<tr>
<td width="100%"><table border="0" width="100%" cellpadding="0">
<tr>
<td width="100%"><p align="center"><strong><font face="隶书" color="#A6A6FF">
xxxx 年 x 月 x 日制作完成</font></strong></td>
</tr>
<tr>
```

```
<td width="100%"><p align="center"><font face="隶书" color="#A6A6FF"><strong>谢谢您的光临</strong></font></td>
</tr>
<tr>
<td width="100%"><p align="center"><strong><font face="隶书" color="#A6A6FF">站长：xxx</font></strong></td>
</tr>
<tr>
<td width="100%"><strong><font face="隶书" color="#A6A6FF">
<marquee border="0" align="middle" scrolldelay="120">
若您需要帮助，请及时找我，联系 E-mail：xxxxx@xxxxx.com</marquee></font></strong></td>
</tr>
</table>
</td>
</tr>
</table>
</body>
</html>
```

该文档在 IE 中的运行效果如图 6-2 所示。

(1) <html></html>元素表示了这个名为 HTML 的文档，即网页。

(2) <head></head>元素用来标明当前文档的若干信息。例中，<head></head>中插入的 title 和 meta 元素分别给 head 元素指明了标题（“意境”）以及所用的字符集(gb2312)。

(3) <title></title>元素给文档起个标题，<meta>元素说明 HTML 所使用的一些信息。

注意：meta 元素不要与 head 元素混淆，meta 元素一般包括在 head 元素中。

(4) 4 个表格元素是 HTML 中最主要的元素。它能解决在排版上遇到的众多问题，例如，文字与图像对齐。<table></table>是定义表格的元素。

(5) <tr></tr>是用来定义表行的元素。在表格中有几对此元素就表示当前表格中有几行。

(6) <td></td>表示一行中单元格的元素。一行中有几对此元素，就有几个单元格。

(7) <th></th>用来定义表头，但此元素现在已经不常用到了。因此，不多作介绍。

(8) 元素规定了字体运用的方式，它有 3 个属性：size、color 和 face，分别代表了字体的大小，颜色及哪种字体。上面的网页中这段代码<font face="隶书" size="6"

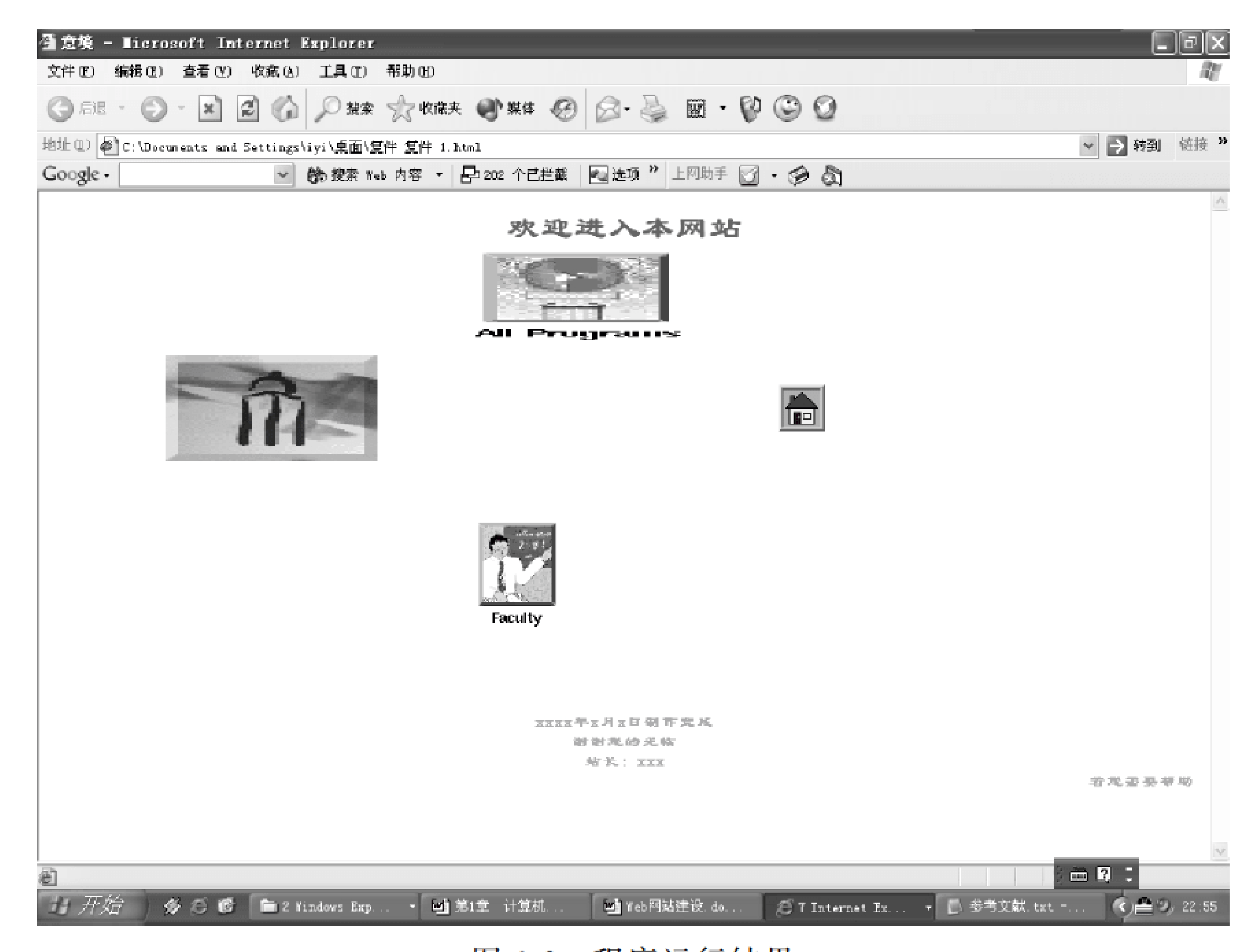


图 6-2　程序运行结果

color="#(可以省略)FF00FF">欢迎进入本网站它表示了"欢迎进入本网站"这 8 个文字，用隶书六号粗(代表粗字体)、紫红色字体在网页中显示出来。另外，color="#FF00FF" 代码中的"#"可以省略。

(9) <img>是专门设置图片属性的元素。

(10) <a href>是一个超链接的元素。在 href 后面写下欲连接的网址，在<a href>与<a>之间写入文字或插入图片，就完成了超链接。

(11) <marquee></marquee>是 HTML 语言的高级技术运用元素。用它可以实现 Web 中文字的滚动效果，使网页更具有动态魅力。这个元素支持以下几个属性：

(12) direction 指定文字的滚动方向，例如，<marquee direction=right>就是指文字从左向右滚动。除了 right，还可以用 left(从右到左)、up(自下往上)或 down(由上朝下)来设定文字的方向。

(13) behavior 指定文字的滚动方式。它有 3 个对象：scroll、slide、alternate。这 3 个对象分别代表了环绕滚动、滚动一次和来回滚动。其中，环绕滚动(即 scroll)是滚动方式(behavior)的默认值。例中的"<marquee border="0" align="middle" scrolldelay="120">若你需要帮助，请及时找我，联系 E-mail：xxx@xxx.com</marquee>"这段代码就指明了文字以默认值 scroll 的方式进行滚动。

（14）loop 指定了文字滚动的循环次数。当 loop=－1 或 loop=infinite 时，表明文字滚动是无限循环。

（15）scrolldelay 指文字滚动的速度。它的单位是毫秒。再看此代码“<marquee border=″0″ align =″ middle″ scrolldelay =″ 120″ > 若你需要帮助，请及时找我，联系 E-mail：xxx @ xxx. com</marquee>”，其中的“scrolldelay =″ 120″”表示文字滚动速度为 120ms。

（16）align 是滚动文字的对齐属性也就是所处的位置。它有 top(对齐上方)、middle(对齐中部)和 bottom(对齐下方)3 个对象。上段代码中的“align=″middle″”则明确了文字的位置是在中部。另外，此元素不仅能够用在 marquee 中，而且在其他元素中也经常用到，如 table、td 等。它们的用法与含义与 marquee 是相同的。

6.2 网页制作工具

在大多数情况下，在创建站点时并不需要开发人员使用 HTML 标记进行设计，因为在网页制作工具软件中，通过“所见即所得”的技术，对 HTML 进行处理，开发人员只须简单地进行界面操作，就能完成网页制作。本节就将介绍几个常用的网页及素材制作工具软件。

（1）Flash 用于设计网络动画，使原本单调的网页变得生动鲜活，它已经慢慢成为网页动画制作的标准，成为一种新兴的技术发展方向。

（2）Fireworks 提供专业网络图形设计和制作方案，支持位图和矢量图。通过它，可以编辑网络图形和动画。同时它能实现网页的无缝连接，与其他图形程序、各 HTML 编辑也能密切配合，为用户一体化的网络设计方案提供支持。

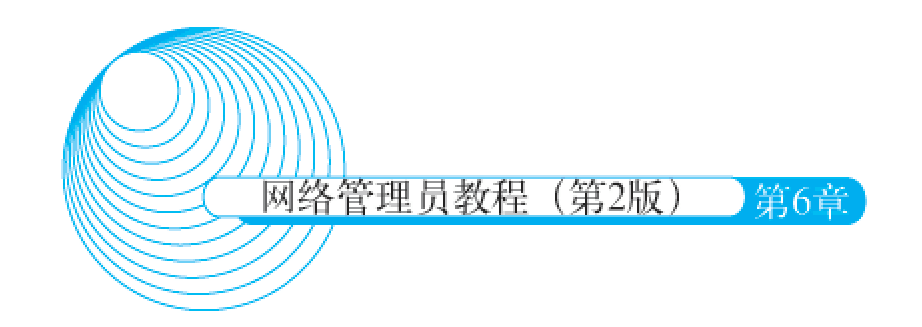
（3）Dreamweaver 是一个所见即所得的主页编辑工具，Dreamweaver 具有强大的功能和简洁的界面，几乎所有的简单对象的属性都可以在属性面上进行修改。

（4）Adobe Photoshop 是数字图像处理软件中最优秀的软件之一，它可以任意设计、处理、润饰各种图像，是网页美术设计理想的数字图像处理软件。

6.2.1 Flash 简介

1. Flash 概述

Flash 是 Macromedia 公司的一个的网页交互动画制作工具。与 gif 和 jpg 不同，用 flash 制作出来的动画是矢量的，不管怎样放大、缩小，它还是清晰可见。用 flash 制作的文档很小，便于在因特网上传输，而且它采用了流技术，只要下载一部分，就能欣赏动画，而且能够一边播放一边传送数据。交互性更是 flash 动画的迷人之处，可以通过单击按钮、选择菜单来控制动画的播



放。正是有了这些优点，才使 flash 日益成为网络多媒体的主流。

2. Flash 工作环境

如图 6-3 所示的是 Flash 的基本工作环境。

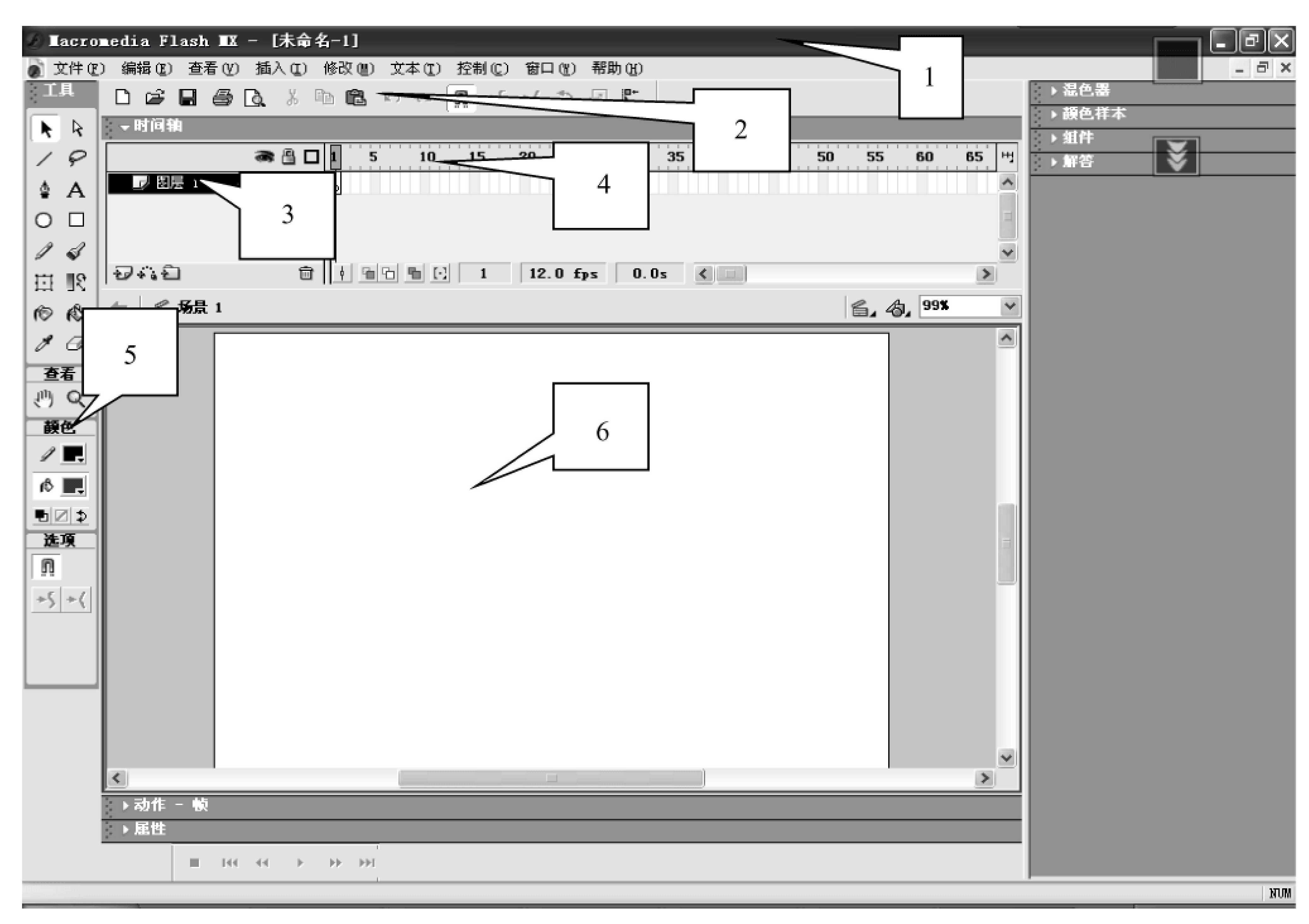


图 6-3　Flash 的基本工作环境

(1) 标题栏：当前程序自动给出了一个文件名称为[无标题-1]，在“保存”文件时要改为一个有意义的文件名称。

(2) 标准工具栏(Standard Toolbar)：列出了大部分最常用的文件操作。如打印、剪贴板、撤销和重做、修改器以及控制舞台放大比例的图标和选项等，便于进行更为快捷的操作。

(3) 图层面板：自动有一个黑色的“图层 1”，其上有 3 个按钮，图层面板用来控制图层的添加、删除、选中等操作。

(4) 时间轴窗口(Timeline)：它可以调整电影的播放速度，并把不同的图形作品放在不同图层的相应帧里，以安排电影内容播放的顺序。

(5) 绘图工具栏(Drawing Toolbar)：其上放置了可供图形和文本编辑的各种工具，用这些工具可以绘图、选取、喷涂、修改以及编排文字，还有些工具可以改变查看工作区的方式。在选

择了某一工具时，它所对应的修改器(Modifier)也会在工具条下面的位置出现，修改器的作用是改变相应工具对图形处理的效果。

(6) 舞台(Stage)：就是工作区，是最主要的可编辑区域。在这里可以直接绘图，或者导入外部图形文件进行安排编辑，再把各个独立的帧合成在一起，生成电影作品。

3. Flash 的特点

(1) 可进行矢量图形处理。计算机显示的图片要么是矢量图像，要么是点阵图像。一般像照片、特效字之类颜色复杂的图形是用点阵图来存贮的，而像卡通画、工程样图等仅由线条和色块组成的图形则是用矢量图来表示的。对于点阵图形，为了减小其文件大小，常采用各种方法来压缩它们，这其中有不损失图形信息的无损压缩和丢掉一些不重要信息的有损压缩。矢量图形是用一些数学公式来描述图形中的点或曲线。矢量图形不仅可以存储平面图形，还可以存储三维立体图形。Flash 允许创建压缩的矢量图形，并使它“动”起来。Flash 还允许输入或者模拟由其他程序生成的矢量或点阵图形。

(2) 采用流播放技术。视音频文件一般都较大，所以需要的存储容量也较大；同时由于网络带宽的限制，下载常常要花数分钟甚至数小时。在网络上传输视音频等多媒体信息目前主要有下载和流式传输两种方案。Flash 采用的流播放技术使得动画可以边播放边下载，从而缓解了网页浏览者焦急的等待。流式传输时，声音、影像或动画等多媒体由视音频服务器向用户计算机连续、实时地传送，用户不必等到整个文件全部下载完毕，而只需几秒或数十秒的启动延时即可进行观看。当声音等多媒体在客户机上播放时，文件的剩余部分将在后台从服务器内继续下载。流式不仅使启动延时成十倍、百倍地缩短，而且不需要太大的缓存容量。

(3) 文件占用的存储空间小。Flash 通过使用关键帧和图符使得所生成的动画(.swf)文件非常小，几 K 字节的动画文件已经可以实现许多生动的动画效果。

所谓图符(Symbol)就是使用绘图工具创建的可重复使用的图形。当把一个图符放到工作区或另一个图符中时，就创建了一个该图符的实例(Instance)，也就是说实例是图符的实际应用。图符的运用可以缩小文档的尺寸，这是因为不管创建了多少个实例，Flash 在文档中只保存一份副本。同样，运用图符可以加快动画播放的速度，用于网页中更是如此，因为对于同一图符的多个实例，浏览器只须下载一次就够了。

在图符的使用中还要注意，修改实例的属性不会影响到图符，但编辑图符将会修改所有与其相关的实例，因为图符和实例之间的联系是单向的。

图符存放在图库窗口中。在 Flash 中，图符分为 3 类。

① 图形类(Graphics)：该图符用标识，用于静态的图形和创建受主影像时间轴控制的可重复使用的动画片断。交互式的控制和音效不能作用于图形符号的序列动画中。

② 按钮类(Button)：标识为，用于创建在影像中对标准的鼠标事件(如单击、滑过或移离等)作出响应的交互式按钮。首先定义与不同的按钮状态相关联的图形，然后给按钮符号的实例指定 actions。

③ 电影片断类(Movie Clip)：用来标识，用于创建可独立于主影像时间轴播放的及可重复使用的动画片断。电影片断就像主影像中的独立小电影，它可以包含交互式控制、音效，甚至可以包含其他的电影片断实例。电影片断的实例也可以放到一个按钮符号的时间轴上来创建动态按钮，可以用电影片断图符实现当鼠标移至按钮上方时按钮发生持续动态变化的效果。

(4) 具有强大的动画编辑功能。强大的动画编辑功能使得设计者可以随心所欲地设计出高品质的动画，通过 ACTION 和 FS COMMAND 可以实现交互性，使 Flash 具有更大的设计自由度，另外，它与当今最流行的网页设计工具 Dreamweaver 配合默契，可以直接嵌入网页的任一位置，非常方便。

(5) 可使音乐、动画和声效融合一体。越来越多的人已经把 Flash 作为网页动画设计的首选工具，并且创作出了许多令人叹为观止的动画(电影)效果。而且 Flash 可以支持 MP3 的音乐格式，这使得加入音乐的动画文件也能占用少量的空间。

Flash 中的艺术作品。Flash 提供了广泛的创造艺术作品或者从其他程序输入艺术作品的方法，可以通过使用绘画工具、染色工具来创建对象，并可以修改现存对象的属性。也可以输入由其他程序生成的矢量图像或点阵图像，然后在 Flash 中对这些输入的图像进行修正。

Flash 动画。所谓 Flash 动画，就是改变对象的形状、大小、色彩、透明度、旋转或者其他对象属性，最易理解的就是对象在舞台上的位移。FLASH 动画分两类，逐帧动画和区间动画。逐帧动画要求为每一个帧创建一个独立的画像，而区间动画仅要求创建动画的开始帧和结束帧，并适当指使 FLASH 自动生成这两个帧之间的所有帧。也可以使用 SET PROPERTY 行为，在电影中创建动画。

Flash 交互电影。所谓 Flash 交互电影，是指观众可以使用键盘或鼠标操作来跳转到电影的其他部分、移动对象、在表格里填写数据，或者执行其他许许多多的操作。交互电影是通过使用 ACTION SCRIPT 设置动作来产生的。

6.2.2 Fireworks 简介

1. Fireworks 概述

Fireworks 是一种专门针对 Web 图像设计而开发的软件。Fireworks 简化了图像设计流程，是一个将矢量图像处理和位图图像处理合二为一的应用程序，因此可以直接在位图图像状态和矢量图像状态之间进行切换，避免了图像在多个应用程序之间的来回迁移。利用 Fireworks，可

以对矢量图像应用在位图图像上才能应用的各种技术和效果，同样，在位图图像上，也可以充分利用矢量图像的编辑优势。

Fireworks 是一个全功能的 Web 设计工具。利用 Fireworks，不仅可以生成静态的图像，还可以直接生成包含 HTML 和 JavaScript 代码的动态图像，甚至可以编辑整幅的网页。例如，可以在 Fireworks 中直接生成各种风格的动态按钮或轮替（Rollover）图像，或是生成图像映像热区（Hotspot）和切片（Slice）。在将图像导出到网页中时，Fireworks 会自动将相应的 HTML 和 JavaScript 代码放置到网页中的正确位置上，从而实现丰富多彩的网页动态效果，避免了用户学习 HTML 和 JavaScript 的麻烦。利用 Fireworks 所生成的图像，色彩完全符合 Web 标准，在设计时是什么颜色，在网页中显示图像时就是什么颜色。

需要指出的是，Fireworks 是基于计算机屏幕的图像处理软件，而不是基于出版印刷的图像处理软件，因此其中可编辑的图像分辨率远远低于印刷图像所需要的分辨率。

2．Fireworks 工作环境

1）文件窗口

Fireworks 的文件窗口上有 4 个标签，如图 6-4 所示。在文件窗口中，可以同时编辑和预览图像，可以同时预览 4 种不同的优化设定所产生的效果，选择最理想的一种设定。



图 6-4　Fireworks 文件窗口

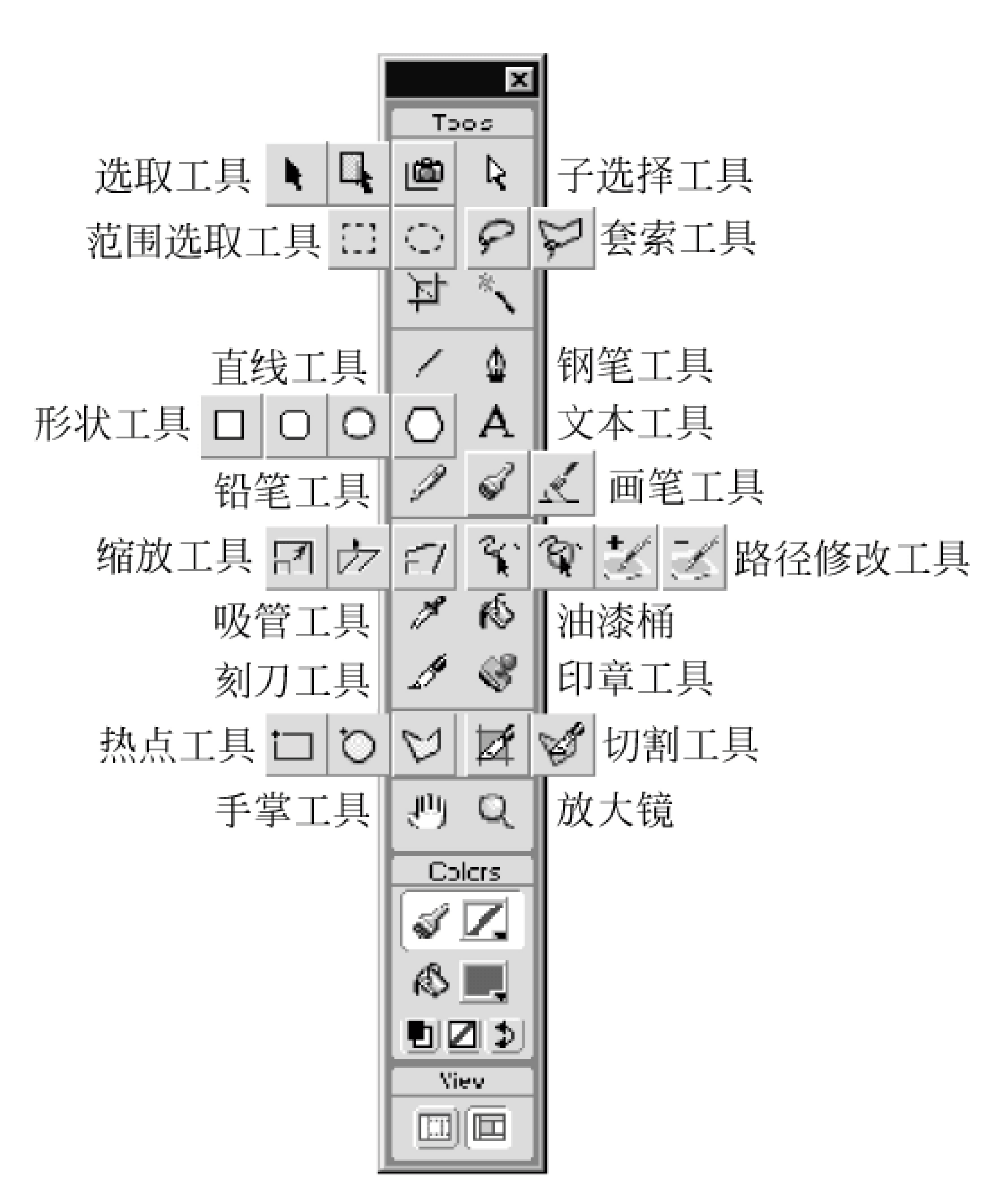
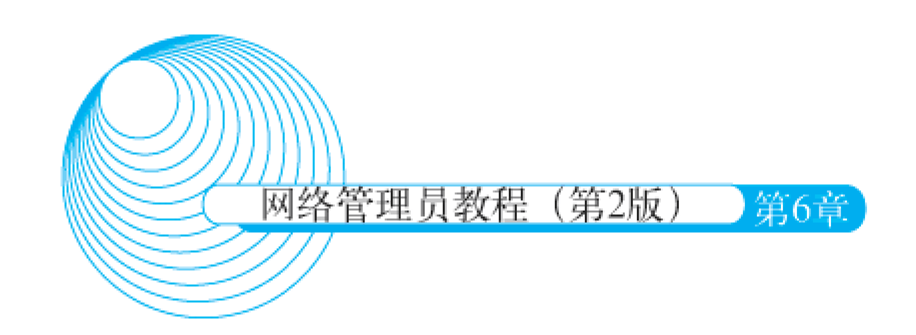


图 6-5　Fireworks 工具条



2）工具条

工具条上包括各种选择、创建、编辑图像的工具，如图 6-5 所示。有的工具按钮的右下角有一个小三角，说明该工具还有几种不同的形式，按住这个工具不放就能显示其他形式。

3）矢量模式与位图模式

Fireworks 可以进行矢量模式与位图模式的编辑，在默认状态下，fireworks 在打开时是处于位图模式下，所绘制的图形是作为矢量对象来处理的。在编辑它们时，会看到是在修改构成矢量图形的路径，如图 6-6 所示。

可以打开或是输入位图，可以对构成位图的像素进行编辑，在处于位图状态下时，画布被带斜纹的框包围着，如图 6-7 所示。

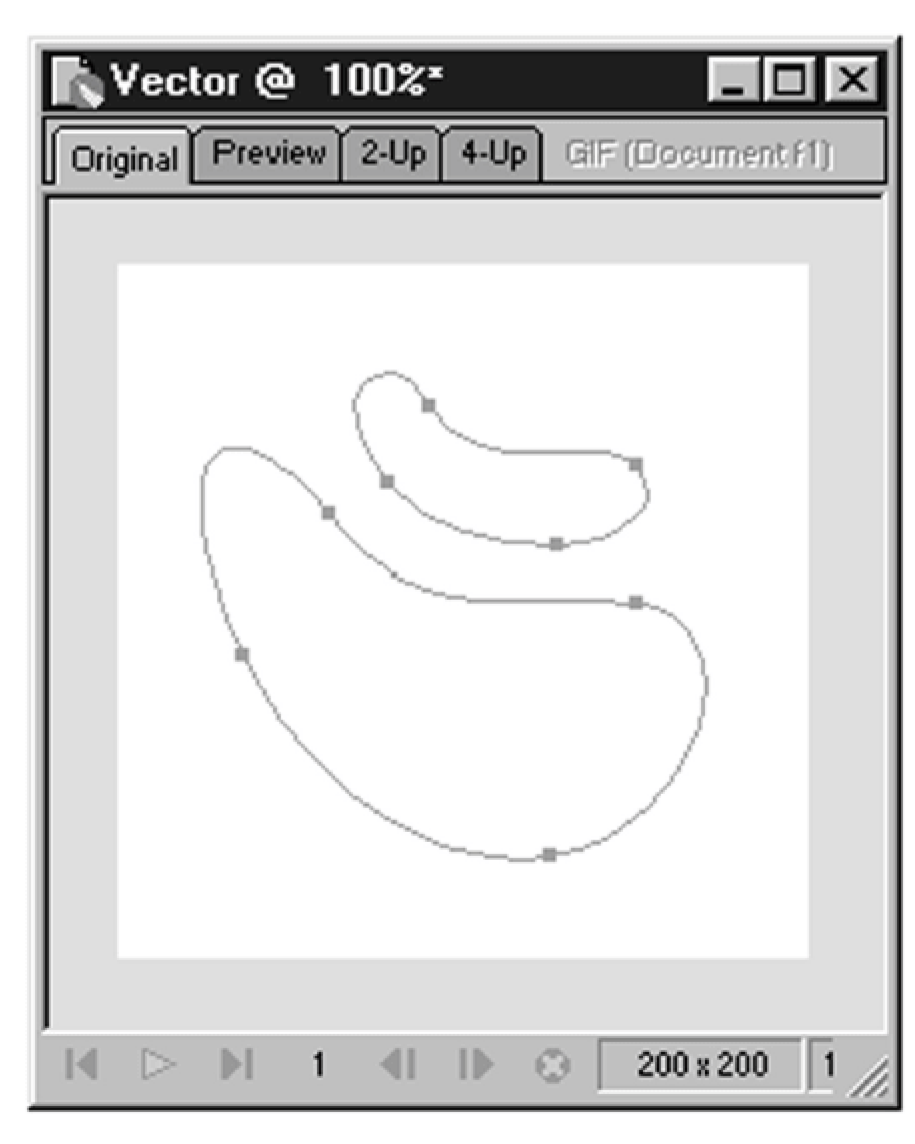


图 6-6　矢量模式



图 6-7　位图模式

4）浮动面板

Fireworks 的浮动面板包括有 Layer（图层）、Frames（帧）、Color Mixs（颜色混合）、Behavior（行为）、Optimize（优化）和 Object（对象）等。

在工作中可能会发现有些面板经常会用到，可以把工作起来最方便的面板排列方式保存起来，使用菜单命令 command→panel layout，如果下次要调出这种排列方式只要在 command→panel layout set 的子菜单内选择就行。

在工作区的右下角有一排快速启动栏，单击快速启动按钮就可以很迅速地调出相应的浮动面板，如图 6-8 所示。

5）库（Library）

库(Library)里储存了可以被重复使用的元素，称为符号(Symbol)，可以创建一个符号或是将已经存在的对象转化为符号，如图6-9所示。

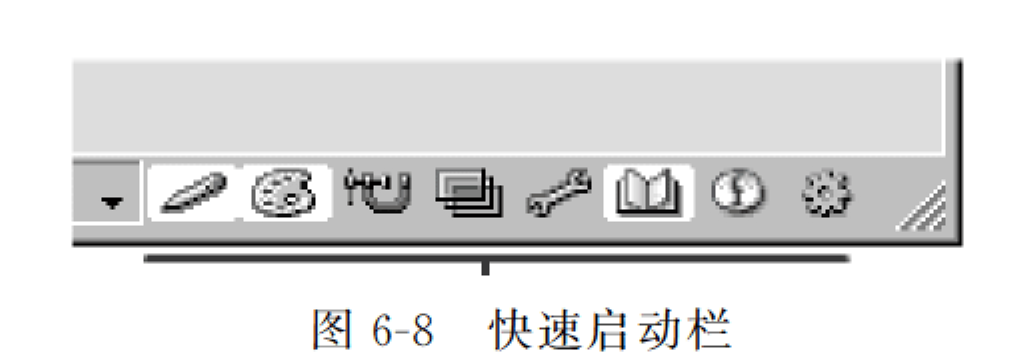


图6-8　快速启动栏

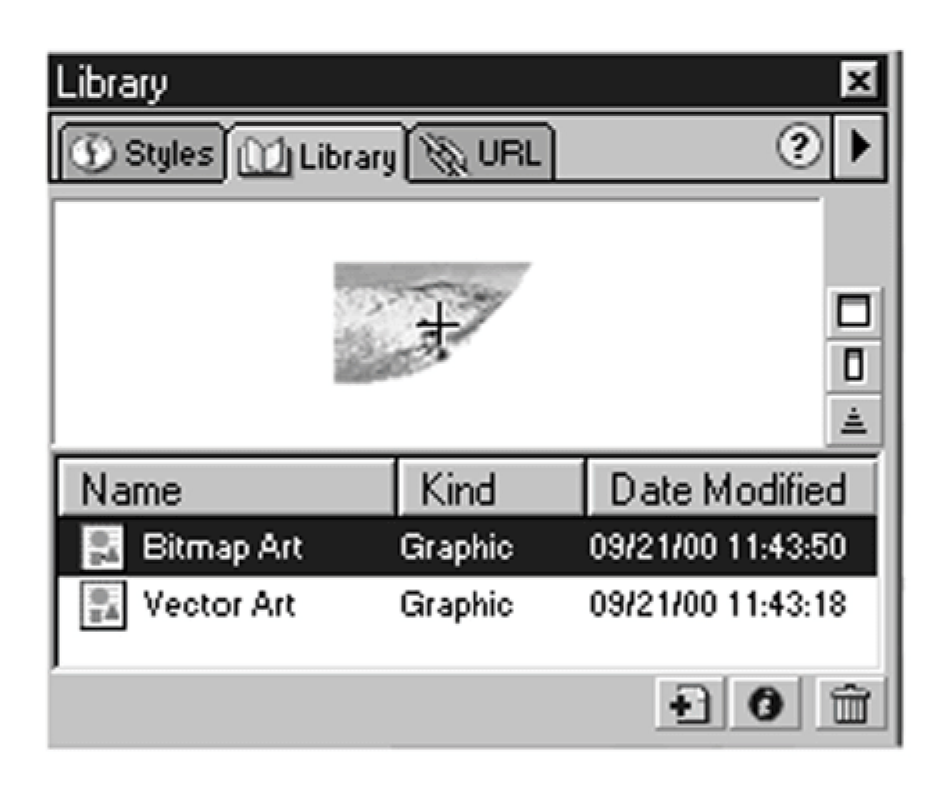


图6-9　库

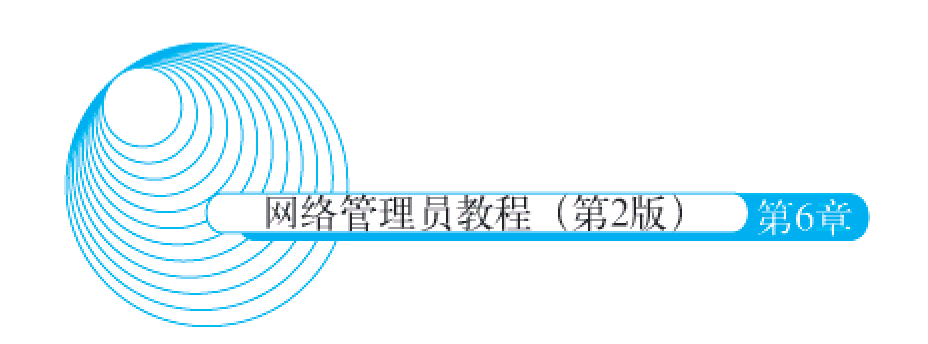
符号分为图像、动画和按钮3种，要调用符号只要把它拖到画布上就可以了，一个符号可以有多个例图(Instance)，如果编辑了符号，那么画布上所有的例图都会改变。

3. Fireworks的特点

(1) 采用图像映像技术，显示的效果好。图像映像是Web中经常使用的一种技术，这种技术的原理是将一幅完整的图像在逻辑上分割为不同的区域(这种区域称作热区)，并将每个热区的坐标记录在网页的源代码中。通过编辑代码，可以为每个热区指派不同的链接路径，使得在浏览网页时，单击图像的不同区域，即可跳转到不同的地方。由于这种方式没有造成图像在视觉上的割裂，因此显示的效果相当好。

(2) 采用切片技术获得较高的下载速度。切片和图像映像类似，都是将图片分割为不同的区域，区别在于图像映像始终作为一幅完整的图像存在，因此如果图像过大，在网页中载入图像会耗费比较多的时间。而利用切片技术，可以将一幅大图像分割为多个小的碎片，以获得较高的下载速度。利用切片进行的分割是真正的分割，它实际上已经将原先的完整图片分割成多个不同的小图片。在网页中，这些小图片被分别放置在HTML表格中的不同单元格里，从而在视觉上以一幅完整图片的形式显示。如果要用手工分割图片的方法设置切片，操作将是非常烦琐复杂的，而在Fireworks中设置切片非常轻松，因为Fireworks提供定位线和切片工具，帮助分割图像，并且会自动根据图像切片的大小，自动构建HTML表格。

(3) 构建按钮和轮替图像。在Fireworks中，可以快速构建多种风格的按钮。利用Fireworks，还可以实现按钮外观的动态改变，轮替图像按钮就是按钮外观动态改变的一种具体应用。所谓轮替，指的是将鼠标移动到按钮上时，按钮的外观发生变化，而将鼠标移出按钮范围



时，按钮外观又变回原先默认外观的这种机制。按钮编辑器可以快速高效地构建 JavaScript 轮替图像按钮，还可以构建包含多个按钮的导航条。

(4) 利用 Fireworks 的样式(Style)特性，可以为图像快速应用一些设置好的艺术效果，这些效果附着于图像元素之上，并且可以在保持原先图像元素本身的条件下任意改换。例如，可以设置图像的投影、发光和浮雕效果，或是设置文字的纹理材质和三维效果等。

(5) Fireworks 是一个将矢量处理和位图处理有机结合的应用程序，因此它可以在处理图像的同时，保持图像元素本身的独立性和可编辑性，所有的效果都是附着在元素身上的，可以被任意替换。利用 Fireworks 中的多种工具，如各种路径工具或位图工具，可以方便快捷地构建动画 GIF 图像。

(6) Fireworks 还支持符号(Symbol)、实例(Instance)和插帧(Tweezing)等特性。所谓符号，指的是具有独立身份的图形元素，在图像中多次复制该图形元素，就构成了实例。一旦在图像中改变了符号本身，它在图像中的所有实例都会相应发生变化，利用这种特性，可以快速地改变整个图像中相同的内容。利用插帧特性，可以快速地在符号和实例之间添加中间帧(也称关键帧)，从而改变动画的过程。

(7) 利用 Fireworks，可以以"图像＋文字"的方式构建完整的 Web 页面，然后再将它导出为真正的"HTML＋图像"的形式。

(8) Fireworks 具有强大的图像优化特性。在 Fireworks 的工作环境中，可以对每个切片进行优化，甚至允许对不同的切片实行不同的优化方式，或以不同的图像文件格式存储。

6.2.3 Dreamweaver 简介

1. Dreamweaver 概述

Dreamweaver 是 Macromedia 公司推出的一个所见即所得的主页编辑工具，Dreamweaver 以简洁的界面和强大的功能著称。在 Dreamweaver 中，几乎所有的简单对象的属性都可以在属性面上进行修改。翻转图片、导航按钮、E-mail 链接、日期、Flash 动画、Shockwave 动画、Java Applet、ActiveX 等对象也可以通过对象面板插入到 Dreamweaver 中。程序使用浮动窗口，设计人员可以用鼠标单击的方式插入图像、表格、表单、Applet、脚本语言等各种对象，这方面延续了所见即所得的编写方式，同时程序也提供对代码的编辑，包括样式表和脚本 JavaScript。Dreamweaver 是第一套针对专业网页开发者特别开发的可视化网页设计工具软件。

2. Dreamweaver 工作环境

启动 Dreamweaver，会看到如图 6-10 所示的画面。Dreamweaver 的界面有许多的窗口分布在上面，最大的空白区域是文档窗口，也是制作过程中 HTML 页面的显示窗口。

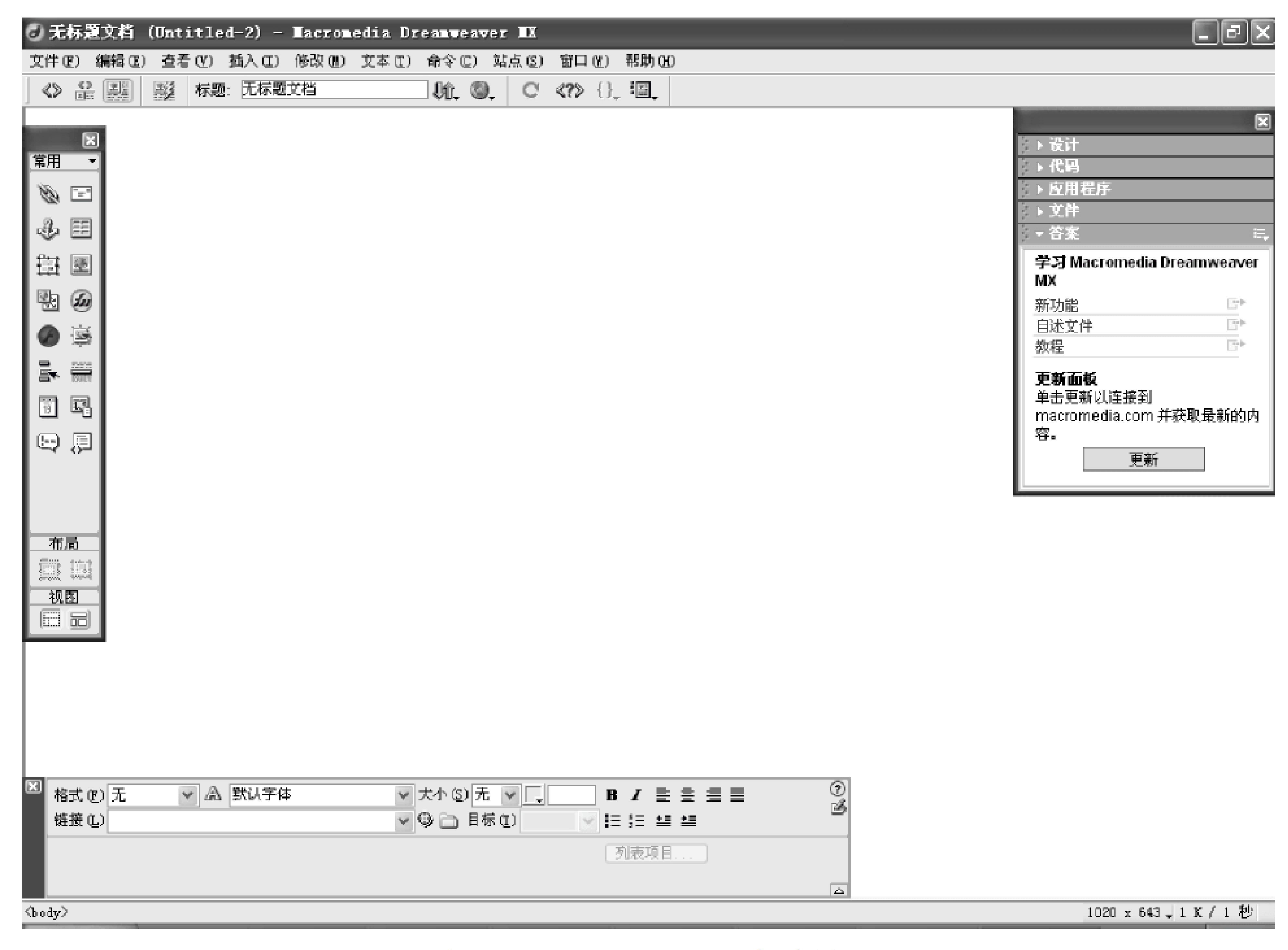


图 6-10　Dreamweaver 启动界面

1）主菜单

Dreamweaver 的主菜单共分 10 大类：文件、编辑、查看、插入、修改、文本、命令、站点、窗口、帮助。作用分别为文件管理、选择区域文本编辑、观察物件、插入元素、修改页面元素、文本操作、附加命令项、命令、站点管理、窗口切换和联机帮助。

2）文档工具栏

文档工具栏如图 6-11 所示，从左到右分别是：切换到代码窗口、切换到代码和设计混合窗口、切换到设计窗口、页面标题、文件管理、预览和在浏览器中改错、参考、代码导航和查看选项。

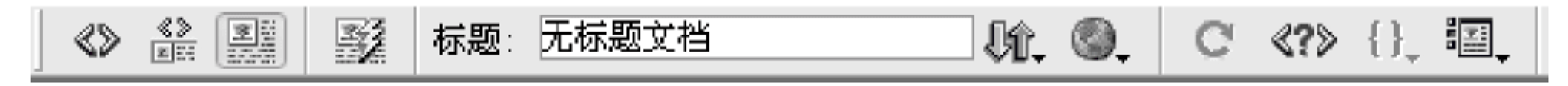
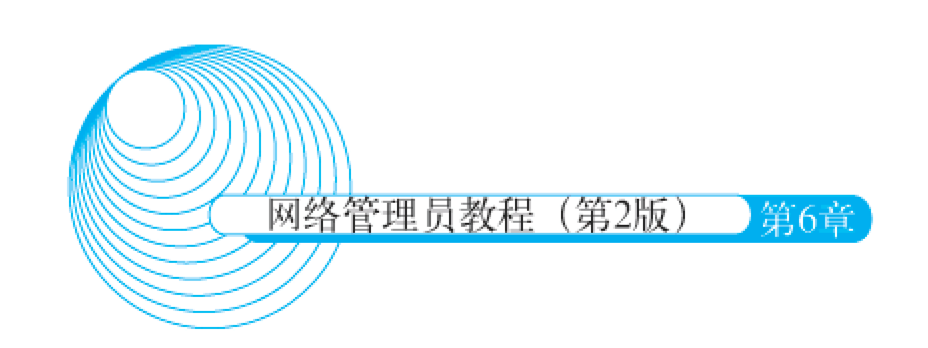


图 6-11　文档工具栏

3）属性面板

属性面板(Properties)比较灵活，变化比较多，它随着选择对象不同而改变，属性菜单完全是随选择区域决定的。比如选择了一幅图像，那么属性面板上将出现图像的相应属性，如果是表



格的话，它相应的会变化成表格的相应属性。

注意：属性面板中的图标，单击后将出现更多的扩展属性。单击图标将关闭扩展属性，返回原始状态。

属性面板集成了 Modify 和 Text 菜单的选项，不过图像属性的修改在主菜单中是找不到的，只能打开其属性面板进行操作。

文本状态下的属性面板如图 6-12 所示。

图像状态下的属性面板如图 6-13 所示。

表格状态下的属性面板如图 6-14 所示。



图 6-12　文本状态下的属性面板

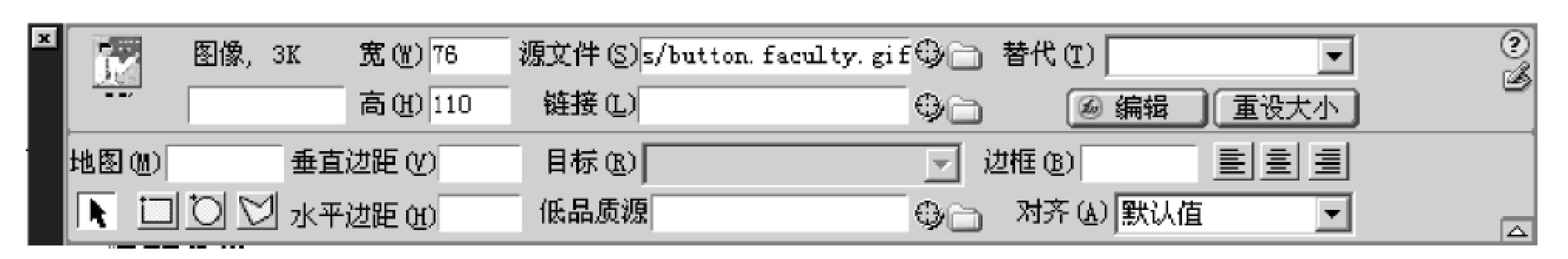


图 6-13　图像状态下的属性面板

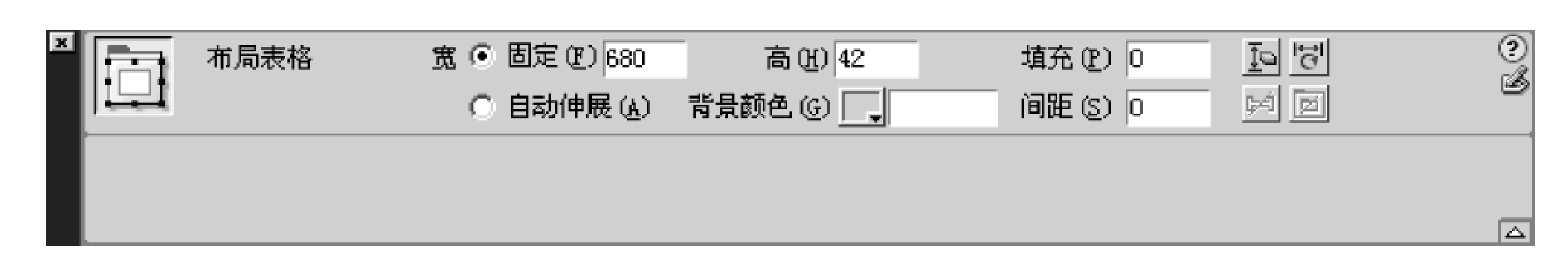


图 6-14　表格状态下的属性面板

4）对象面板

对象面板集成了 Dreamweaver 主菜单中 Insert 中的选项，它的对象全是插入对象，而且图标直观，如图 6-15。

5）状态栏

状态栏的左边一部分是显示当前光标区的代码情况，可以用鼠标任意选定其中的一句代码，单击后所选中的代码会加粗，如图 6-16 所示。

状态栏右边剩下的部分如图 6-17 所示。该部分由 3 部分组成，从左到右分别表示当前的用户界面的分辨率，单击后可调整为需要的分辨率；中间的部分显示目前编辑的文档（包括图像

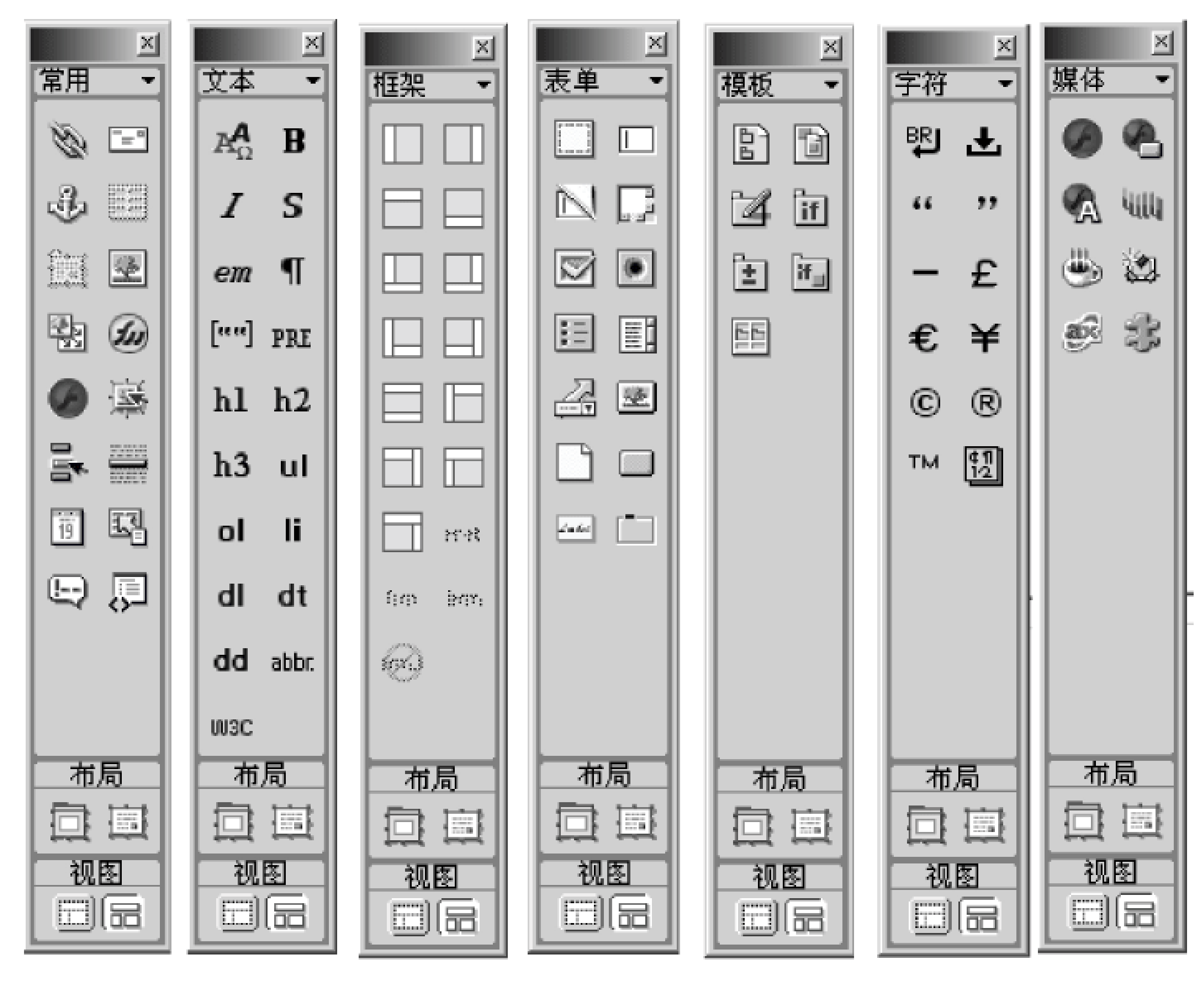


图 6-15　对象面板

等）共有多少 kB，并根据设定的传输速率计算出相应的下载时间，使用户可以随时掌握自己页面的总容量，作出相应的决定。最右边的一部分是 Launcher（快速启动档）。



图 6-16　表格状态下的属性面板一

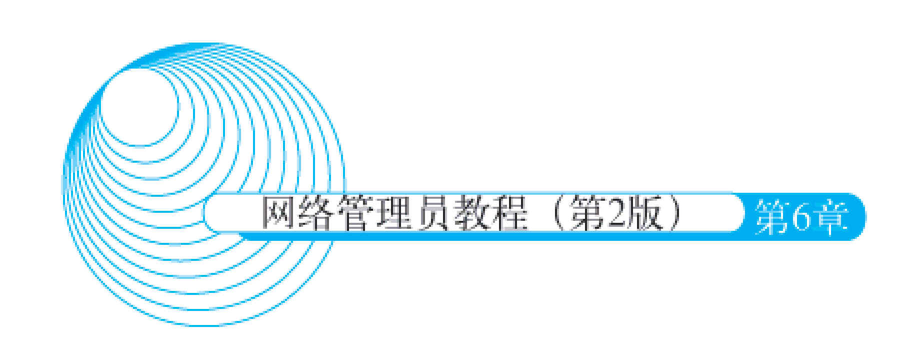


图 6-17　表格状态下的属性面板二

3. Dreamweaver 的特点

（1）Dreamweaver 提供可视化网页开发，同时不会降低 HTML 原码的控制。Dreamweaver 提供的 Roundtrip HTML 功能，可以准确无误地切换于视觉模式与惯用的原码编辑器。当编辑既有的网页时，Dreamweaver 会尊重在其他编辑器作出的原码，不会任意地改变它。而在使用 Dreamweaver 的视觉性编辑环境时，可以在 HTML 监视器上同步地看到 Dreamweaver 产生的原始码，而若想要在视觉式编辑模式和原始码编辑模式之间跳换的话，只须单击一下相应的窗口。

（2）Dreamweaver 支持跨浏览器的 Dynamic HTML，阶层式样式窗体、绝对坐标定位以及 JavaScript 的动画。Dreamweaver 利用 JavaScript 和 DHTML 语言代码实现网页元素的动作和交互操作。在这方面超过了 FrontPage、Hotdog、Homesite 等著名网页编写软件。Dynamic HTML、直觉式时间轴接口以及 JavaScript 行为库，可在不需要程序的情况下让 HTML 组件运



动起来。全网站内容管理的方式克服了逐页更新管理的缺点。

（3）Dreamweaver 提供行为和时线两种控件来进行动画处理和产生交互式响应，这也是这个软件的优势所在。行为空间提供交互式操作，时线控件使设计人员可以像制作视频一样来编辑网页。

（4）和 Macromedia 公司其他软件的完美协作也是 Dreamweaver 的一大特色。Dreamweaver 中可以直接插入 Fireworks 中导出的 HTML 代码，设置 Dreamweaver 中的图像也可以直接使用 Fireworks 进行编辑和优化。

6.2.4 Photoshop 简介

1. Photoshop 概述

Adobe Photoshop 是数字图像处理软件中最优秀的软件之一，它可任意设计、处理、润饰各种图像，是美术设计、摄影和印刷专业人员理想的数字图像处理工具软件。Photoshop 被誉为目前最强大的图像处理软件之一，具有十分强大的图像处理功能。而且，Photoshop 具有广泛的兼容性，采用开放式结构，能够外挂其他处理软件和图像输入输出设备。

Photoshop 为美术设计人员提供了无限创意空间，可以从一幅现成的图像开始，通过各种图像组合，在图像中任意添加图像，为作品增添艺术魅力。Photoshop 的所有绘制成果均可以输出到彩色喷墨打印机、激光打印机上。

对于印刷人员，Adobe Photoshop 提供了高档专业印刷前期作业系统，通过扫描、修改图像，在 RGB 模式中预览 CMYK 四色印刷图像，在 CMYx 模式中对颜色进行编辑，产生高质量的单色、双色、三色和四色调图像。

2. Photoshop 工作环境

Photoshop 界面如图 6-18 所示。

（1）标题栏：标题栏显示 Adobe Photoshop 的字样和图标。

（2）菜单栏：菜单栏显示的是 Photoshop 菜单命令。共包括文件、编辑、图像、图层、选择、滤镜、视图、窗口和帮助 9 个菜单。

（3）工具箱：工具箱中列出 Photoshop 中的常用工具。利用工具箱中的工具可以选择、绘制、编辑和查看图像，选择前景和背景色以及更改屏幕显示模式。大多数工具都有相关的笔刷大小和选项调板，用以限定工具的绘画和编辑效果。

（4）控制面板：控制面板列出 Photoshop 许多操作的功能设置和参数设置。利用这些设置可以进行各种操作。

（5）状态栏：状态栏显示当前打开图像的信息和当前操作的提示信息。



图 6-18　Photoshop 界面

（6）图像窗口：图像窗口显示图像。窗口上方显示图像文件的名称、大小比例和色彩模式。

3．Photoshop 的特点

（1）支持多种图像格式。Photoshop 支持的图像格式包括 PSD、EPS、DCS、TIF、JEPG、BMP、PCX、FLM、PDF、PICT、GIF、PNG、IFF、FPX、RAW 和 SCT 等 20 多种。利用 Photoshop 可以将某种格式的图像另存为其他格式，以达到特殊的需要。

（2）支持多种色彩模式。Photoshop 支持的色彩模式包括位图模式、灰度模式、RGB 模式、CMYK 模式、Lab 模式、索引颜色模式、双色调模式和多通道模式等，并且可以实现各种模式之间的转换。另外，利用 Photoshop 还可以任意调整图像的尺寸、分辨率及画布的大小。既可以在不影响分辨率的情况下改变图像尺寸，又可以在不影响图像尺寸的情况下增减分辨率。

（3）提供了强大的选取图像范围的功能。利用矩形、椭圆面罩和套索工具，可以选取一个或多个不同尺寸、形状的选取范围。磁性套索工具可以根据选择边缘的像素反差，使选取范围紧贴要选取的图像。利用魔术棒工具或“颜色范围”命令可以根据颜色来自动选取所要部分。配合多种快捷键的使用，可以实现选取范围的相加、相减、交叉和反选等效果。

(4) 可以对图像进行各种编辑，如移动、复制、粘贴、剪切、清除等。如果在编辑时出了错误，还可以进行无限次地撤销和恢复。Photoshop 可以对图像进行任意的旋转和变形，例如按固定方向翻转和旋转，或对图像进行拉伸、倾斜、扭曲和制造透视效果等。

(5) 可以对图像进行色调和色彩的调整，使色相、饱和度、亮度、对比度的调整变得简单容易。Photoshop 可以单独对某一选取范围进行调整，也可以对某一种选定颜色进行调整。使用"色彩平衡"命令可以在彩色图像中改变颜色的混合。使用"色阶"和"曲线"命令可以分别对图像的高光、暗调和中间调部分进行调整，这是传统的绘画技巧难以达到的效果。

(6) 提供了绘画功能。使用喷枪工具、笔刷工具、铅笔工具、直线工具，可以绘制各种图形。通过自行设定的笔刷形状、大小和压力，可以创建不同的笔刷效果。利用渐变工具可以产生多种渐变效果。加深和减淡工具可以有选择地改变图像的曝光度。海绵工具可以选择性地增减色彩的饱和程度。模糊、锐化和涂抹工具可以产生特殊效果的图像作品。使用图章工具可以修改图像，并可复制图像中的某一部分内容到其他图像的指定位置。

(7) 使用 Photoshop，用户可以建立普通图层、背景层、文本层、调节层等多种图层，并且方便地对各个图层进行编辑。用户可以对图层进行任意的复制、移动、删除、翻转、合并和合成，可以实现图层的排列，还可以应用添加阴影等操作制造特技效果。调整图层可在不影响图像的同时，控制图层的透明度和饱和度等图像效果。文本层可以随时编辑图像中的文本。用户还可以对不同的色彩通道分别进行编辑。利用蒙版可以精确地选取范围，进行存储和载入操作。

(8) Photoshop 共提供了将近 100 种的滤镜，每种滤镜各不相同。用户可以利用这些滤镜实现各种特殊效果，如利用"风"滤镜可以增加图像动感，利用"浮雕"滤镜可以制作浮雕效果，利用"水波"滤镜可以模拟水波中的倒影。另外，Photoshop 还可以使用很多其他与之配套的外挂滤镜。

6.3 动态网页的制作

早期的 Web 主要是静态页面的浏览，由 Web 服务器使用 HTTP 协议将 HTML 文档从 Web 服务器传送到用户的 Web 浏览器上。它适合于组织各种静态的文档类型元素如图片、文字及文档间的链接。

Web 技术发展的第二阶段是生成动态页面。随着三层 Client/Server 结构和 CGI 标准、ISAPI 扩展、动态 HTML 语言、Java/JDBC 等技术的出现，产生了可以供用户交互的动态 Web 文档，HTML 页除了能显示静态信息外，还能够作为信息管理中客户与数据库交互的人机界面。动态网页技术主要依赖服务器端编程，包括 CGI 版本、Server-API 程序(包括 NSAPI 和 ISAPI)、JavaServerlets 以及服务器端脚本语言。

服务端脚本编程方式试图使编程和网页联系更为紧密，并使它以相对更简单、更快速的方

式运行。服务器端脚本的思想是创建与 HTML 混合的脚本文件或模板，当需要的时候由服务器来读它们，然后服务器分析处理脚本代码，并输出由此产生的 HTML 文件。图 6-19 显示了这个过程。

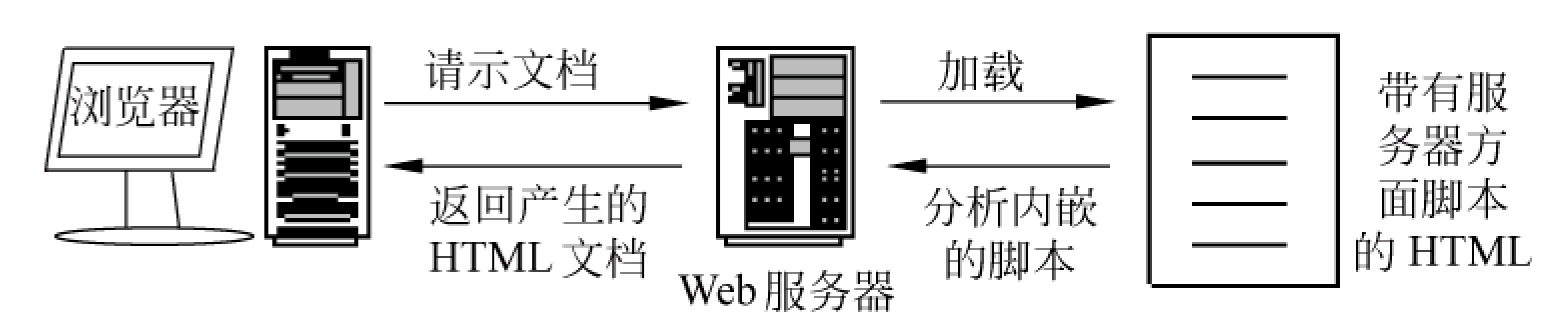


图 6-19　服务器端脚本的分析过程

服务器脚本环境有许多，其中最流行的几种包括 ASP（Active Server Pages）、JSP（Java Server Pages）、ColdFusion 、PHP 等，它们的主要区别仅在于语法上。每一种技术与其他技术相比差别不大，因此在它们之间作出选择往往是出于自己的偏爱。所有这样技术与更先进的服务器端编程如服务器 API 相比，其执行速度相对较慢。可以弥补性能的是该项技术相对比较简单。

6.3.1　ASP

1. ASP 简介

1）什么是 ASP

ASP 从字面上说，包含 3 个方面的含义：

（1）Active。ASP 使用了 Microsoft 的 ActiveX 技术。它采用封装程序调用对象的技术，以简化编程和加强程序间合作。ASP 本身封装了一些基本组件和常用组件，有很多公司也开发了很多实用组件。只要在服务器上安装这些组件，通过访问组件，就可以快速、简易地建立 Web 应用。

（2）Server。ASP 运行在服务器端，这样就不必担心浏览器是否支持 ASP 所使用的编程语言。ASP 的编程语言可以是 VBScript 和 JavaScript。VBScript 是 VB 的一个简集，会使用 VB 的人可以很方便的快速上手。然而 Netscape 浏览器不支持客户端的 VBScript，所以最好不要在客户端使用 VBScript。而在服务器端，则无须考虑浏览器的支持问题。Netscape 浏览器也可以正常显示 ASP 页面。

（3）Pages。ASP 返回标准的 HTML 页面，可以在常用的浏览器中显示。浏览者查看页面源文件时，看到的是 ASP 生成的 HTML 代码，而不是 ASP 程序代码。

由此看出，ASP 是在 IIS（Internet Information Server）下开发 Web 应用的一种简单、方便的编程工具。在了解了 VBScript 的基本语法后，只须搞清楚各个组件的用途、属性、方法，就可以轻松编写出自己的 ASP 页面。

2）ASP 的特点

（1）使用 VBScript、JScript 等简单易懂的脚本语言，结合 HTML 代码，即可快速地完成网站的应用程序。

（2）使用普通的文本编辑器，如 Windows 的记事本，即可进行编辑设计。

（3）不需要 compile 编译，容易编写，可在服务器端直接执行。

（4）与浏览器无关(Browser Independence)。用户端只要使用可执行 HTML 码的浏览器，即可浏览 Active Server Pages 所设计的网页内容。Active Server Pages 所使用的脚本语言(VBScript、JScript)均在 Web 服务器端执行，用户端浏览器不需要执行这些脚本语言。

（5）Active Server Pages 能与任何 ActiveX scripting 语言相容。除了可使用 VBScript 或 JScript 语言来设计外，还通过 plug-in 的方式，使用由第三方所提供的其他脚本语言，譬如 REXX、Perl、Tcl 等。脚本引擎是处理脚本程序的 COM(Component Object Model)物件。

（6）Active Server Pages 的源程序，不会被传到客户浏览器，因而可以避免所写的源程序被他人剽窃，同时也提高了程序的安全性。

（7）可使用服务器端的脚本来产生客户端的脚本。

（8）物件导向(Object-oriented)。

（9）ActiveX Server Components(ActiveX 服务器元件)具有无限可扩充性。可以使用 Visual Basic、Java、Visual C++ 、COBOL 等编程语言来编写需要的 ActiveX Server Component。

3）ASP 编程环境

与一般的程序不同，ASP 程序无须编译，ASP 程序的控制部分是使用 VBScript、JScript 等脚本语言来设计的。当执行 ASP 程序时，脚本程序将一整套命令发送给脚本解释器(即脚本引擎)，由脚本解释器进行翻译并将其转换成服务器所能执行的命令。当然，同其他编程语言一样，ASP 程序的编写也遵循一定的规则，如果想使用某种脚本语言编写 ASP 程序，那么服务器上必须要有能够解释这种脚本语言的脚本解释器。当安装 ASP 时，系统提供了两种脚本语言：VBSrcipt 和 JavaScript，而 VBScript 则是系统默认的脚本语言。

ASP 程序其实是以扩展名为.asp 的纯文本形式存在于 Web 服务器上的，所以可以用任何文本编辑器打开它，ASP 程序中可以包含纯文本、HTML 标记以及脚本命令。只须将.asp 程序放在 Web 服务器的虚拟目录下(该目录必须要有可执行权限)，即可以通过 WWW 的方式访问 ASP 程序。

所谓脚本，是由一系列的脚本命令组成的，如同一般的程序，脚本可以将一个值赋给一个变量，可以命令 Web 服务器发送一个值到客户浏览器，还可以将一系列命令定义成一个过程。要编写脚本，必须要熟悉至少一门脚本语言，如 VBScript。脚本语言是一种介乎于 HTML 和诸如 Java、Visual Basic、C++ 等编程语言之间的一种特殊的语言，尽管它更接近后者，但它却不具有编程语言复杂、严谨的语法和规则。ASP 所提供的脚本运行环境可支持多种脚本语言，如 JScript、Perl，这给 ASP 程序设计者提供了发挥余地。ASP 的出现使得 Web 设计者不必在为客户浏览器是否支持而担心，实际上就算在同一个.asp 文件中使用不同的脚本语言，也无须为此

担忧，因为所有的一切都将在服务器端进行，客户浏览器得到的只是一个程序执行的结果，只须在.asp 中声明使用不同的脚本语言即可。

2. ASP 内嵌对象

ASP 提供了可在脚本中使用的内嵌对象。这些对象使用户更容易收集那些通过浏览器请求发送的信息，响应浏览器以及存储用户信息，从而使对象开发摆脱了很多繁琐的工作。内嵌对象不同于正常的对象。在利用内嵌对象的脚本时，不需要首先创建一个实例。在整个网站应用中，内嵌对象的所有方法、集合以及属性都是自动可访问的。

一个对象由方法、属性和集合构成，其中对象的方法决定了这个对象可以做什么。对象的属性可以读取，它描述对象状态或者设置对象状态。对象的集合包含了很多和对象有关系的键和值的配对。例如：书是一个对象，这个对象包含的方法决定了可以怎样处理它。书这个对象的属性包括页数、作者等。对象的集合包含了许多键和值的配对，对书而言，每一页的页码就是键，那么值就是对应于该页码的这一页的内容。

1）Request 对象

Request 对象为脚本提供了当客户端请求一个页面或者传递一个窗体时，客户端提供的全部信息。这包括能指明浏览器和用户的 HTTP 变量，在这个域名下存放在浏览器中的 Cookie，任何作为查询字符串而附于 URL 后面的字符串或页面的<form>段中的 HTML 控件的值，同时也提供使用 Secure Socket Layer(SSL)或其他加密通信协议的授权访问，以及有助于对连接进行管理的属性。

(1）Request 对象的集合：Request 对象提供了 5 个集合，可以用来访问客户端对 Web 服务器请求的各类信息。如表 6-1 所示。

表 6-1 Request 对象的集合

集合名称	说明
Client Certificate	当客户端访问一个页面或其他资源时，用来向服务器表明身份的客户证书的所有字段或条目的数值集合，每个成员均是只读
Cookies	根据用户的请求，用户系统发出的所有 Cookie 的值的集合，这些 Cookie 仅对相应的域有效，每个成员均为只读
Form	METHOD 的属性值为 POST 时，所有作为请求提交的<form>段中的 HTML 控件单元的值的集合，每个成员均为只读
QueryString	依附于用户请求的 URL 后面的名称/数值对或者作为请求提交的且 METHOD 属性值为 GET(或者省略其属性)的，或<form>中所有 HTML 控件单元的值，每个成员均为只读
ServerVariables	随同客户端请求发出的 HTTP 报头值，以及 Web 服务器的几种环境变量的值的集合，每个成员均为只读

（2）Request 对象的属性：Request 对象唯一的属性及说明如表 6-2 所示，它提供关于用户请求的字节数量的信息，它很少用于 ASP 页，通常关注指定值而不是整个请求字符串。

表 6-2　Request 对象的属性及说明

属性	说明
Total Bytes	只读，返回由客户端发出的请求的整个字节数量

（3）Request 对象的方法：Request 对象唯一的方法及说明如表 6-3 所示，它允许访问从一个<form>段中传递给服务器的用户请求部分的完整内容。

表 6-3　Request 对象的方法及说明

方法	说明
Binary Read（count）	当数据作为 POST 请求的一部分发往服务器时，从客户请求中获得 count 字节的数据，返回一个 Variant 数组。如果 ASP 代码已经引用了 Request．Form 集合，这个方法就不能用。同样，如果用了 Binary Read 方法，就不能访问 Request．Form 集合

2）Response 对象

用来访问服务器端所创建的并发回到客户端的响应信息。为脚本提供 HTTP 变量，指明服务器、服务器的功能、关于发回浏览器的内容的信息以及任何将为这个域而存放在浏览器里新的 Cookie。它也提供了一系列的方法用来创建输出，例如：Response. Write 方法。

（1）Response 对象的集合：Response 对象只有一个集合，如表 6-4 所示，该集合设置希望放置在客户系统上的 Cookie 的值，它直接等同于 Request. Cookie 集合。

表 6-4　Response 对象的集合及说明

集合名称	说明
Cookie	在当前响应中，发回客户端的所有 Cookie 的值，这个集合为只写

（2）Response 对象的属性：Response 对象也提供一系列的属性，可以读取和修改，使响应能够适应请求。这些由服务器设置，不需要设置它们。需要注意的是，当设置某些属性时，使用的语法可能与通常所使用的有一定的差异。这些属性如表 6-5 所示。

表 6-5　Response 对象的属性及说明

属性	说明
Buffer＝True|False	读/写，布尔型，表明由一个 ASP 页所创建的输出是否一直存放在 IIS 缓冲区，直到当前页面的所有服务器脚本处理完毕或 Flush、End 方法被调用。在任何输出(包括 HTTP 报头信息)送往 IIS 之前这个属性必须设置。因此在.asp 文件中，这个设置应该在＜％@ LANGUAGE＝…％＞语句后面的第一行
CacheControl "setting"	读/写，字符型，设置这个属性为 Public 则允许代理服务器缓存页面，属性如为 Private，则禁止代理服务器缓存的发生
Charest＝"value"	读/写，字符型，在由服务器为每个响应创建的 HTTP Content-Type 报头中附上所用的字符集名称
Content Type ＝ "MIME-type"	读/写，字符型，指明响应的 HTTP 内容类型，标准的 MIME 类型(例如 text/xml 或者 Image/gif)。假如省略，表示使用 MIME 类型 text/html，内容类型告诉浏览器所期望内容的类型
Expires minutes	读/写，数值型，指明页面有效的以分钟计算的时间长度，假如用户请求其有效期满之前的相同页面，将直接读取显示缓冲中的内容，这个有效期间过后，页面将不再保留在私有(用户)或公用(代理服务器)缓冲中
Expires Absolute ＃date [time]＃	读/写，日期/时间型，指明当一个页面过期和不再有效时的绝对日期和时间
Is Client Connected	只读，布尔型，返回客户是否仍然连接和下载页面的状态标志。在当前的页面已执行完毕之前，假如一个客户转移到另一个页面，这个标志可用来中止处理
PICS ("PICS-Label-string")	只写，字符型，创建一个 PICS 报头并将之加到响应中的 HTTP 报头中，PICS 报头定义页面内容中的词汇等级，如暴力、性、不良语言等
Status＝"Code message"	读/写，字符型，指明发回客户的响应的 HTTP 报头中表明错误或页面处理是否成功的状态值和信息。例如 200 OK 和 404 Not Found

(3) Response 对象的方法：Response 对象提供一系列的方法，如表 6-6 所示，允许直接处理为返给客户端而创建的页面内容。

3) ASP 的 Application 对象成员概述

Application 对象是在为响应一个 ASP 页的首次请求而载入 ASP DLL 时创建的，它提供了存储空间用来存放变量和对象的引用，可用于所有的页面，任何访问者都可以打开它们。

(1) Application 对象的集合：Application 对象提供了两个集合，可以用来访问存储于全局应用程序空间中的变量和对象。集合及说明如表 6-7 所示。

表 6-6　Response 对象的方法及说明

方法	说明
AddHeader ("name","content")	通过使用 name 和 Content 值，创建一个定制的 HTTP 报头，并增加到响应之中。不能替换现有的相同名称的报头。一旦已经增加了一个报头就不能被删除。这个方法必须在任何页面内容(即 text 和 HTML)被发往客户端前使用
AppendToLog ("string")	当使用 W3C Extended Log File Format 文件格式时，对于用户请求的 Web 服务器的日志文件增加一个条目。至少要求在包含页面的站点的 Extended Properties 页中选择 URI Stem
BinaryWrite (SafeArray)	在当前的 HTTP 输出流中写入 Variant 类型的 Safe Array，而不经过任何字符转换。对于写入非字符串的信息，例如定制的应用程序请求的二进制数据或组成图像文件的二进制字节，是非常有用的
Clear ( )	当 Response . Buffer 为 True 时，从 IIS 响应缓冲中删除现存的缓冲页面内容。但不删除 HTTP 响应的报头，可用来放弃部分完成的页面
End ( )	让 ASP 结束处理页面的脚本，并返回当前已创建的内容，然后放弃页面的任何进一步处理
Flush ( )	发送 IIS 缓冲中所有当前缓冲页给客户端。当 Response . Buffer 为 True 时，可以用来发送较大页面的部分内容给个别的用户
Redirect ("URL")	通过在响应中发送一个 302 Object Moved 的 HTTP 报头，指示浏览器根据字符串 URL 下载相应地址的页面
Write ("string")	在当前的 HTTP 响应信息流和 IIS 缓冲区写入指定的字符，使之成为返回页面的一部分

表 6-7　Application 对象的集合及说明

集合	说明
Contents	没有使用<OBJECT>元素定义的存储于 Application 对象中的所有变量(及它们的值)的一个集合。包括 Variant 数组和 Variant 类型对象实例的引用
StaticObjects	使用<OBJECT>元素定义的存储于 Application 对象中的所有变量(及它们的值)的一个集合

(2) Application 对象的方法：Application 对象的方法允许删除全局应用程序空间中的值，控制在该空间内对变量的并发访问。方法及说明如表 6-8 所示。

(3) Application 对象的事件：Application 对象提供了在它启动和结束时触发的两个事件，如表 6-9 所示。

表 6-8　Application 对象的方法及说明

方法	说明
Contents. Remove ("variable_name")	从 Application. Content 集合中删除一个名为 variable_name 的变量
Contents. RemoveAll()	从 Application. Content 集合中删除所有变量
Lock( )	锁定 Application 对象，使得只有当前的 ASP 页面对内容能够进行访问。用于确保通过允许两个用户同时地读取和修改该值的方法而进行的并发操作不会破坏内容
Unlock ( )	解除对在 Application 对象上的 ASP 网页的锁定

表 6-9　Application 对象的事件及说明

事件	说明
OnStar	当 ASP 启动时触发，在用户请求的网页执行之前以及任何用户创建 Session 对象之前。用于初始化变量、创建对象或运行其他代码
OnEnd	当 ASP 应用程序结束时触发。在最后一个用户会话已经结束并且该会话的 OnEnd 事件中的所有代码已经执行之后发生。其结束时，应用程序中存在的所有变量被取消

4）ASP 的 Session 对象成员概述

独特的 Session 对象是在每一位访问者从 Web 站点或 Web 应用程序中首次请求一个 ASP 页时创建的，它将保留到默认的期限结束（或者由脚本决定中止的期限）。它与 Application 对象一样提供一个空间用来存放变量和对象的引用，但只能供目前的访问者在会话的生命期中打开的页面使用。

（1）Session 对象的集合：Session 对象提供了两个集合，可以用来访问存储于用户的局部会话空间中的变量和对象。这些集合及说明如表 6-10 所示。

表 6-10　Session 对象的集合及说明

集合	说明
Contents	存储于这个特定 Session 对象中的所有变量和其值的一个集合，并且这些变量和值没有使用<OBJECT>元素进行定义。包括 Variant 数组和 Variant 类型对象实例的引用
StaticObjects	通过使用<OBJECT>元素定义的、存储于这个 Session 对象中的所有变量的一个集合

（2）Session 对象的特性：Session 对象提供了 4 个属性。这些属性及说明如表 6-11 所示。

表 6-11 Session 对象的属性及说明

属性	说明
CodePage	读/写，整型。定义用于在浏览器中显示页内容的代码页(Code Page)。代码页是字符集的数字值，不同的语言和场所可能使用不同的代码页。例如，ANSI 代码页 1252 用于美国英语和大多数欧洲语言。代码页 932 用于日文字
LCID	读/写，整型。定义发送给浏览器的页面地区标识(LCID)。LCID 是唯一的标识地区的一个国际标准缩写，例如，2057 定义当前地区的货币符号是'£'。LCID 也可用于 Format Currency 等语句中，只要其中有一个可选的 LCID 参数。LCID 也可在 ASP 处理指令<%…%>中设置，并优先于会话的 LCID 属性中的设置
Session ID	只读，长整型。返回这个会话的会话标识符，创建会话时，该标识符由服务器产生。在父 Application 对象的生存期内是唯一的，因此当一个新的应用程序启动时可重新使用
Timeout	读/写，整型。为这个会话定义以分钟为单位的超时周期。如果用户在超时周期内没有进行刷新或请求一个网页，该会话结束。在各网页中根据需要可以修改。默认值是 10min，在使用率高的站点上该时间应更短

（3）Session 对象的方法：Session 对象允许从用户级的会话空间删除指定值，并根据需要终止会话。Session 对象的方法及说明如表 6-12 所示。

表 6-12 Session 对象的方法及说明

方法	说明
Contents. Remove ("variable_name")	从 Session. Content 集合中删除一个名为 variable_name 的变量
Contents. RemoveAll()	从 Session. Content 集合中删除所有变量
Abandon()	当网页的执行完成时，结束当前用户会话并撤销当前 Session 对象。但即使在调用该方法以后，仍可访问该页中的当前会话的变量。当用户请求下一个页面时将启动一个新的会话，并建立一个新的 Session 对象

（4）Session 对象的事件：Session 对象提供了在启动和结束时触发的两个事件，如表 6-13 所示。

表 6-13 Session 对象的事件及说明

事件	说明
OnStart	当 ASP 用户会话启动时触发，在用户请求的网页执行之前。用于初始化变量、创建对象或运行其他代码
OnEnd	当 ASP 用户会话结束时触发。从用户对应用程序的最后一个页面请求开始，如果已经超出预定的会话超时周期则触发该事件。当会话结束时，取消该会话中的所有变量。在代码中使用 Abandon 方法结束 ASP 用户会话时，也触发该事件

5）ASP Server 对象成员概述

Server 对象提供了一系列的方法和属性，在使用 ASP 编写脚本时是非常有用的。最常用的是 Server. CreateObject 方法，它允许在当前页的环境或会话中在服务器上实例化其 COM 对象。还有一些方法能够把字符串翻译成在 URL 和 HTML 中使用的正确格式，这通过把非法字符转换成正确、合法的等价字符来实现。

Server 对象是专为处理服务器上的特定任务而设计的，特别是与服务器的环境和处理活动有关的任务。因此提供信息的属性只有一个，却有 7 种方法用来以服务器特定的方法格式化数据、管理其他网页的执行、管理外部对象和组件的执行以及处理错误。

（1）Server 对象的属性：Server 对象的唯一一个属性用于访问一个正在执行的 ASP 网页的脚本超时值，如表 6-14 所示。

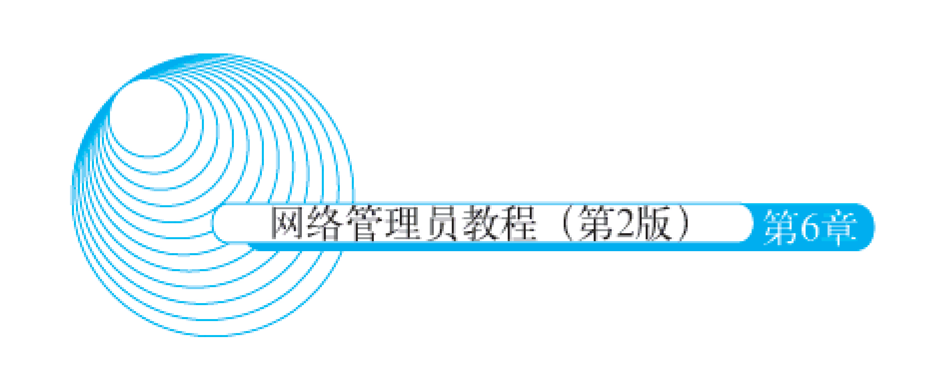
表 6-14　Server 对象的属性及说明

特性	说明
ScriptTimeout	整型，默认值为 90。设置或返回页面的脚本在服务器退出执行和报告一个错误之前可以执行的时间(以秒为单位)。达到该值后将自动停止页面的执行，并从内存中删除包含可能进入死循环的错误的页面或者是那些长时间等待其他资源的网页。这会防止服务器因存在错误的页面而过载。对于运行时间较长的页面需要增大这个值

（2）Server 对象的方法：Server 对象的方法用于格式化数据、管理网页执行和创建其他对象实例，如表 6-15 所示。

表 6-15　Server 对象的方法及说明

方法	说明
CreateObject ("identifier")	创建由 identifier 标识的对象(一个组件、应用程序或脚本对象)的一个实例，返回可以在代码中使用的一个引用。可以用于一个虚拟应用程序(global. asa 页)创建会话层或应用程序层范围内的对象。该对象可以用其 Class ID 来标识，如"{clsid: BD96C556-65A3…37A9}"或一个 ProgID 串来标识，如 ADODB. Connection
Execute("URL")	停止当前页面的执行，把控制转到在 URL 中指定的网页。用户的当前环境(即会话状态和当前事务状态)也传递到新的网页。在该页面执行完成后，控制传递回原先的页面，并继续执行 Execute 方法后面的语句
GetLastError()	返回 ASP ASPError 对象的一个引用，这个对象包含该页面在 ASP 处理过程中发生的最近一次错误的详细数据。这些由 ASP Error 对象给出的信息包含文件名、行号、错误代码等
HTML Encode ("string")	返回一个字符串，该串是输入值 string 的复制，但去掉了所有非法的 HTML 字符，如<、>、& 和双引号，并转换为等价的 HTML 条目，即"<"、">"、"&"、"""等



续表

方法	说明
MapPath("URL")	返回在 URL 中指定的文件或资源的完整物理路径和文件名
Transfer("URL")	停止当前页面的执行，把控制转到 URL 中指定的页面。用户的当前环境（即会话状态和当前事务状态）也传递到新的页面。与 Execute 方法不同，当新页面执行完成时，不回到原来的页面，而是结束执行过程
URL Encode ("string")	返回一个字符串，该串是输入值 string 的复制，但是在 URL 中无效的所有字符，如?、& 和空格，都转换为等价的 URL 条目，即% 3 F、% 2 6 和＋

3．ASP 使用范例

下面是一个 ASP 的例子：

```
<HTML>
<BODY>
<TABLE>
<% Call Callme %>
</TABLE>
<% Call ViewDate %>
</BODY>
</HTML>
<SCRIPT LANGUAGE=VBScript RUNAT=Server>
Sub Callme
    Response. Write "<TR><TD>Call</TD><TD>Me</TD></TR>"
End Sub
</SCRIPT>
<SCRIPT LANGUAGE=JScript RUNAT=Server>
function ViewDate()
{
    var x
    x = new Date()
    Response. Write(x. toString())
}
</SCRIPT>
```

ASP 不同于客户端脚本语言，它有特定的语法，所有的 ASP 命令都必须包含在 <% 和%>之内，例如：<% test="English" %>。ASP 通过包含在<%和%>中的表达式将

执行结果输出到客户浏览器。例如：＜％ ＝test ％＞就是将前面赋给变量 test 的值 English 发送到客户浏览器中，而当变量 test 的值为 Mathematics 时，以下程序：

This weekend we will test ＜％ ＝test ％＞.

在客户浏览器中则显示为：

This weekend we will test Mathematics.

6.3.2 JSP

服务器端动态网页(JSP，Java Server Pages)是由 Sun 公司(Sun Microsystems Inc)倡导、许多公司参与一起建立的一种动态网页技术标准，其在动态网页的建设中有其强大而特别的功能。目前在国外的众多网站特别是涉及电子商务的网站中，已经大量使用了 JSP 技术。

JSP 是在“服务器”建立的动态网页。更明确地说，JSP 能在 Web Server(尤其是 JSWDK)端整合 Java 语言至 HTML 网页的环境中，利用 HTML 网页内含的 Java 程序代码取代原有的 CGI、ISAPI 或者 IDC 的程序，以便执行原有 CGI/WINCGI、ISAPI 的功能。

JSP 技术为创建显示动态生成内容的 Web 页面提供了一个简捷而快速的方法。JSP 技术的设计目的是使得构造基于 Web 的应用程序更加容易和快捷，而这些应用程序能够与各种 Web 服务器、应用服务器、浏览器和开发工具共同工作。

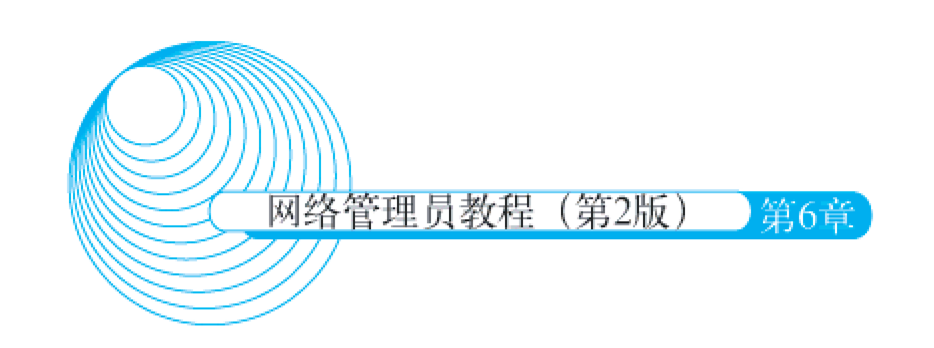
所谓的 JSP 网页(*.jsp)，就是在传统的网页 HTML 文件(*.htm、*.html)中加入 Java 程序片段(Scriptlet)和 JSP 标记(tag)而构成的。Web 服务器在遇到访问 JSP 网页的请求时，首先执行其中的程序片段，然后将执行结果以 HTML 格式返回给客户。程序片段可以操作数据库、重新定向网页以及发送 E-mail 等，这就是建立动态网站所需要的功能。所有程序操作都在服务器端执行，网络上传送给客户端的仅是得到的结果，对客户浏览器的要求最低，可以实现无 Plug-in、无 ActiveX、无 Java Applet，甚至无 Frame。

在 Sun 正式发布 JSP 之后，这种新的 Web 应用开发技术很快引起了人们的关注。JSP 为创建高度动态的 Web 应用提供了一个独特的开发环境。

1. JSP 的特点

JSP 能在 Web Server(尤其是 JSWDK)端整合 Java 语言至 HTML 网页的环境中，然后利用 HTML 网页内含的 Java 程序代码取代原有的 CGI、ISAPI 或者 IDC 的程序，以便执行原有 CGI/WinCGI、ISAPI 的功能。

JSP 的运作模式。相对应于 Client 端(指的是浏览器端的 HTML 文件)内嵌的描述语言，Sun 公司提供的 JSWDK 也支持类似的描述语言，它便是 Java 语言。由于 JSP 放置在 Web 服务器上，它在解析使用者由表单(FM)传送过来的字段数据后，接着通过适当的逻辑生成 HTML



文件，然后传给客户端，使用者看到的是一般符合 HTML 格式的文件内容。因为 JSP 是在 JSWDK 上执行的，所以无论使用的是哪一种平台下的浏览器，皆能看到由 JSP 产生的网页内容。

JSP 与 ASP、PHP 相比有下列优点。

1）内容的生成和显示进行分离

使用 JSP 技术，Web 页面开发人员可以使用 HTML 或者 XML 标识来设计和格式化最终页面。使用 JSP 标识或者小脚本来生成页面上的动态内容（内容是根据请求来变化的，例如请求账户信息或者特定的一瓶酒的价格）。生成内容的逻辑被封装在标识和 JavaBean 组件中，并且捆绑在小脚本中，所有的脚本在服务器端运行。如果核心逻辑被封装在标识和 Java Bean 中，那么其他人，如 Web 管理人员和页面设计者，能够编辑和使用 JSP 页面，而不影响内容的生成。

在服务器端，JSP 引擎解释 JSP 标识和小脚本，生成所请求的内容（例如，通过访问 JavaBean 组件，使用 JDBCTM 技术访问数据库，或者包含文件），并且将结果以 HTML（或者 XML）页面的形式发送回浏览器。这有助于作者保护自己的代码，而又保证任何基于 HTML 的 Web 浏览器的完全可用性。

2）强调可重用的组件

绝大多数 JSP 页面依赖于可重用的、跨平台的组件（JavaBean 或者 Enterprise JavaBean TM 组件）来执行应用程序所要求的更为复杂的处理。开发人员能够共享和交换执行普通操作的组件，或者使得这些组件为更多的使用者或者客户团体所使用。基于组件的方法加速了总体开发过程，并且使得各种组织在他们现有的技能和优化结果的开发努力中得到平衡。

3）采用标识简化页面开发

Java Server Page 技术封装了许多功能，这些功能是在易用的、与 JSP 相关的 XML 标识中进行动态内容生成所需要的。标准的 JSP 标识能够访问和实例化 JavaBean 组件，设置或者检索组件属性，下载 Applet，以及执行用其他方法更难于编码和耗时的功能。

通过开发定制标识库，JSP 技术是可以扩展的。今后，第三方开发人员和其他人员可以为常用功能创建自己的标识库，这使得 Web 页面开发人员能够使用熟悉的工具和如同标识一样的执行特定功能的构件来工作。

JSP 技术很容易整合到多种应用体系结构中，利用现存的工具和技巧，扩展到能够支持企业级的分布式应用。作为采用 Java 技术家族的一部分，以及 Java 2（企业版体系结构）的一个组成部分，JSP 技术能够支持高度复杂的基于 Web 的应用。

4）健壮性与安全性

由于 JSP 页面的内置脚本语言是基于 Java 编程语言的，而且所有的 JSP 页面都被编译成为 Java Serverlet，JSP 页面就具有 Java 技术的所有好处，包括健壮的存储管理和安全习性。

5）良好的移植性

作为 Java 平台的一部分，JSP 拥有 Java 编程语言“一次编写，各处运行”的特点。随着越来越多的供应商将 JSP 支持添加到他们的产品中，可以使用所选择的服务器和工具，而且更改服务器或工具并不影响当前的应用。

6）企业级的扩展性和性能

当与 Java 2 平台，企业版(J2EE)和 Enterprise JavaBean 技术整合时，JSP 页面将提供企业级的扩展性和性能，这对于在虚拟企业中部署基于 Web 的应用是必需的。

2. JSP 程序页面

下面是 JSP 的一个例子，完成打印年、月的日期，并且根据时间使用"Good Morning"和"Good Afternoon"表示欢迎。

```
<HTML>
<%@ page language=="java" imports=="com. wombat. JSP. * " %>
<H1>Welcome</H1>

<P>Today is </P>
<jsp:useBean id=="clock" class=="calendar. jspCalendar" />
<UL>
<LI>Day: <%==clock. getDayOfMonth() %>
<LI>Year: <%==clock. getYear() %>
</UL>

<% if (Calendar. getInstance(). get(Calendar. AM_PM) ==== Calendar. AM) { %>
Good Morning
<% } else { %>
Good Afternoon
<% } %>
<%@ include file=="copyright. html" %>

</HTML>
```

这个页面包含下面这些组件：

(1) 一个 JSP 指示将信息传送到 JSP 引擎。在这个示例中，第一行指出从该页面即将访问的一些 Java 编程语言的扩展的位置。指示被设置在<%@和%>标记中。

(2) 固定模板数据。所有 JSP 引擎不能识别的标识将随结果页面发送。通常，这些标识是 HTML 或者 XML 标识。在上面的例子中包括无序列表(UL)和 H1 标识。

(3) JSP 动作或者标识。这些通常作为标准或定制标识被实现，并且具有 XML 标识的语法。在这个例子中，jsp:useBean 标识实例化服务器端的 Clock JavaBean。

(4) 一个表达式。JSP 引擎计算在＜％＝＝和％＞标记间的所有东西。在上面的列表项中，时钟组件(Clock)的 Day 和 Year 属性值作为字符串返回，并且作为输出插入到 JSP 文件中。在上面的例子中，第一个列表项是日子，第二个是年份。

小脚本是执行不为标识所支持的功能或者将所有的东西捆绑在一起的小的脚本。在上面示例中的小脚本确定现在是上午还是下午，并且据此来欢迎用户。

基于 Java 的小脚本提供了一种灵活的方式以执行其他功能，而不要求扩展的脚本语言。页面作为整体是可读和可理解的，这就使得查找或者预防问题以及共享工作更加容易。

3. JSP 技术的未来

JSP 技术被设计为一个开放的，可扩展的建立动态 Web 页面的标准。开发人员可以使用 JSP 页面来创建可移植的 Web 应用，在不同的 Web 和应用服务器上为不同的场合所运行，而不论采用什么适合本身场合和需要的创建工具。

通过与业界领袖的合作，Sun 保证 JSP 规范是开放的和可移植的。可以使用任何客户机和服务器平台，在任何地方编写和部署它们。将来，工具供应商和其他厂商将通过为专门的功能提供客户化的标识库而扩展平台的功能。

6.3.3 XML

Web 上的文档组织包含了服务器端文档的存储方式、客户端页面的浏览方式以及传输方式。下一代 Web 对文档的组织在数据表达能力、扩展能力、安全性上都提出了新的要求。HTML 已经不能满足当前网络数据描述的需要。1998 年 2 月 10 日 W3C(World Wide Web Consortium)正式公布了 XML1.0 版本。XML(Extensible Markup Language)，即可扩展标记语言，是用于标记电子文件的结构化语言。与 HTML 相比，XML 是一种真正的数据描述语言，它没有固定的标记符号，允许用户自己定义一套适合于应用的文档元素类型，因而具有很大的灵活性。XML 包含了大量的自解释型的标识文本，每个标识文本又由若干规则组成，这些规则可用于标识，使 XML 能够让不同的应用系统理解相同的含义，正是由于这些标识的存在，XML 能够有效地表达网络上的各种知识，也为网上信息交换提供了载体。

1. XML 的特征

XML 与 HTML 相比主要有以下特点：

(1) XML 是元标记语言。HTML 定义了一套固定的标记，每一种标记都有其特定的含义。XML 与之不同，它是一种元标记语言，用户可以自定义所需的标记。

(2) XML 描述的是结构和语义。XML 标记描述的是文档的结构和意义，而不是显示页面元素的格式。简单地说就是文档本身只说明文档包括什么标记，而不是说明文档看起来是什么样的。

(3) XML 文档的显示使用特有的技术来支持。例如，通过使用样式单为文档增加格式化信息。

2. XML 的基本语法

一个格式正规的 XML 文档由 3 个部分组成：一个可选的序言(prolog)、文档的主体(body)和可选的尾声(epilog)。一个 XML 文件通常以一个 XML 声明开始，后面通过 XML 元素来组织 XML 数据。XML 元素包括标记和字符数据。标记用尖括号括起来以便与数据区分开来。尖括号中可以包含一些属性。为了组织数据更加方便、清晰，还可以在字符数据中引入 CDATA 数据块，并可以在文件中引入注释。此外，由于有时需要给 XML 处理程序提供一些指示信息，XML 文件中可以包含处理指示。

一个符合 XML 文档语法规范的 XML 文档是“格式正规”的文档，以下是一份格式正规的 XML 文档：

```
<? xml version="1.0" encoding="GB2312"? >
<? xml-stylesheet href="style.xsl" type="text/xsl"? >
<! -- 以上是 XML 文档的序言部分 -->

<COLLEGE>
    <TITLE>计算机学院</TITLE>
    <LEADER>王志东</LEADER>
    <STU_NUMBER unit="人">3</STU_NUMBER>

    <STUDENT>
      <NAME>李文</NAME>
      <AGE>21</AGE>
      <SEX>男</SEX>
      <CLASS>9902</CLASS>
</STUDENT>
<STUDENT>
      <NAME>张雨</NAME>
      <AGE>20</AGE>
      <SEX>女</SEX>
      <CLASS>9901</CLASS>
```

```
</STUDENT>
<STUDENT>
    <NAME>刘鹏</NAME>
    <AGE>19</AGE>
    <SEX>女</SEX>
    <CLASS>9903</CLASS>
</STUDENT>
</COLLEGE>
<! —— 以上是文档的主体部分，以下是文档的尾声部分 ——>
```

可以看出，XML 文档序言部分从文档的第一行开始，它可以包括 XML 声明、文档类型声明、处理指令等。文档的主体则是由文档根元素所包含的那一部分。XML 尾声部分在文档的末尾，它可以包含注释、处理指令或空白。

接下来分别介绍组成文档的各种要素，以此来阐述 XML 文档的基本语法。

1）声明

一个 XML 文件通常以一个 XML 声明作为开始，XML 声明在文件中是可选内容，可加可不加，但 W3C 推荐加入这一行声明。因此，作为一个良好的习惯，通常把 XML 声明作为 XML 文件的第一行。

XML 声明的作用就是告诉 XML 处理程序："下面这个文件是按照 XML 文件的标准对数据进行置标的"。例如，一个最简单的 XML 声明是这样的：

```
<? xml version = "1.0"? >
```

可以看到，XML 声明由"<?"开始，由"? > "结束。在"<?"后面紧跟着处理指示的名称，在这里是 xml，XML 这 3 个字母不区分大小写。

XML 声明中要求必须指定 version 的属性值。同时，声明中还有两个可选属性：standalone 和 encoding。因此，一个完整的 XML 声明应该是这样的：

```
<? xml version? = "1.0" encoding= "GB2312" standalone? = "no"? >
```

下面来看看这几个属性的具体含义。

（1）version 属性：指明所采用的 XML 的版本号，而且，它必须在属性列表中排在第一位。由于当前的 XML 最新版本是 1.0，所以看到的情况无一例外地都是：version="1.0"。

（2）encoding 属性：所有的 XML 语法分析器都要支持 8 位和 16 位的编码标准。不过，XML 可能支持一个更庞大的编码集合。在 XML 规范中列出了一大堆编码类型。但一般用不到这么多编码，只要知道下面几个常见的编码就可以了：GB2312（简体中文码）、BIG5（繁体中文码）、UTF－8（西欧字符）。

XML 的字符编码标准是 Unicode，因此所有的 XML 解析器都应该提供对 Unicode 编码标

准的支持。该字符编码标准中每个字符用 16 比特表示，可以表示 65 536 个不同的字符。与 Unicode 之前被广泛使用的 ASCII 相比，Unicode 码最大的好处是能够处理多种语言字符。采用哪种编码取决于文件中用到的字符集。如果标记是采用中文书写的，则必须要在声明中加上 encoding ＝"GB2312"的属性。

（3）standalone 属性：表明该 XML 文件是否需要从其他外部资源获取有关标记定义的规范说明，并据此检查当前 XML 文档的有效性。这个属性置的默认值为 no，表示可能有也可能没有这样一个文件。如果该属性置为 yes，说明没有另外一个配套的文件来进行置标声明。

2）元素

当已经写好一个 XML 声明，一个新的 XML 文件就宣告诞生了。而文档的主体则由一个或多个元素组成，元素是 XML 文件内容的基本单元。从语法上讲，元素用标记（tag）进行分隔，一个元素包含一个起始标记和一个结束标记，属性和标记之间的数据内容是可选的，其形式如图 6-20 所示。

<elementNAME(attrName="")>　content　</elementName>

起始标记　　属性　　字符数据　　结束标记

图 6-20　XML 元素

元素可以包含其他元素、字符数据、实体引用、处理指令、注释和 CDATA 部分。这些统称为元素内容（element content）。

位于文档最顶层的一个元素包含了文档中其他所有元素，称为根元素。另外，元素中还可以再嵌套别的元素。需要说明的是，元素之间应正确的嵌套，不能互相交叉。所有元素构成一个简单的层次树，元素和元素之间唯一的直接关系就是父子关系。XML 文档的层次结构如图 6-21 所示。

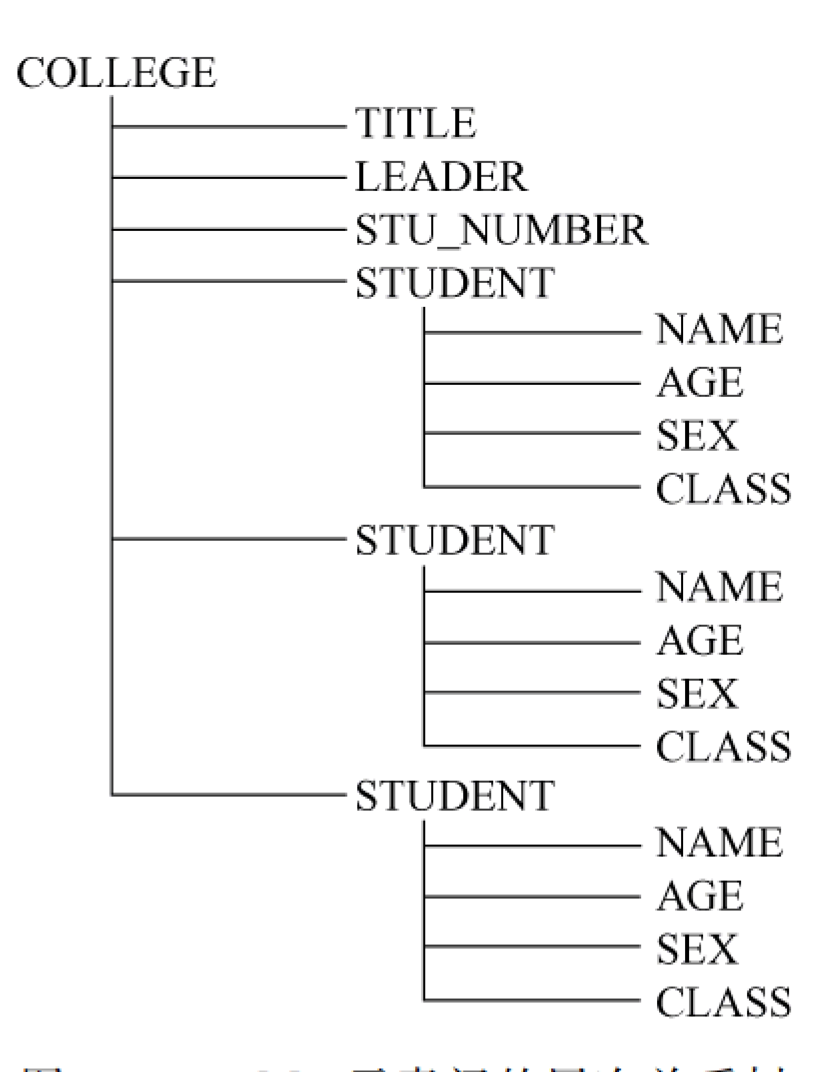


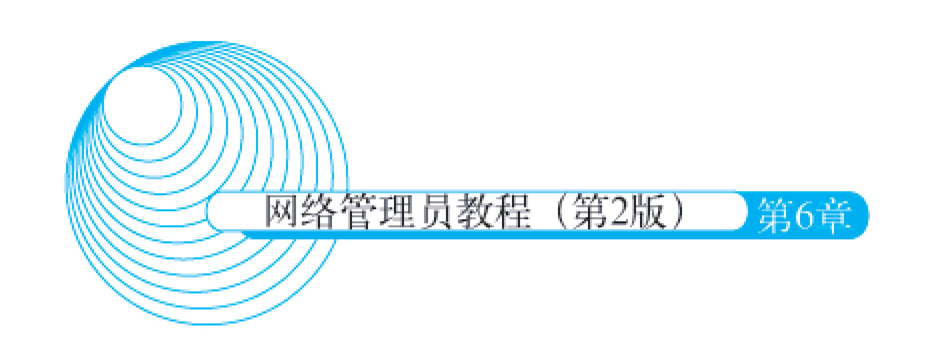
图 6-21　XML 元素间的层次关系树

"置标"是 XML 语言的精髓。因此，标记在 XML 的元素中、乃至整个 XML 文件中，占有举足轻重的位置。XML 的标记和 HTML 的标记在模样上大体相同，除了注释和 CDATA 部分以外，所有符号"<"和符号">"之间的内容都称为标记。其基本形式为：

<标记名（属性名="属性值"）*>

XML 对于标记的语法规定比 HTML 要严格得多。

（1）标记命名要合法。XML 规范中的标识符号命名规则为：标记必须以字母、下划线"_"或冒号":"开头，后跟有效标记命名符号，包括字母、数字、句号"."、冒号":"、下划线"_"或连字符"-"，但是中间不能有空



格，而且任何标记不能以 xml 起始。另外，最好不要在标记的开头使用冒号，尽管它是合法的，但可能会带来混淆。在 XML1.0 标准中允许使用任何长度的标记，不过，现实中的 XML 处理程序可能会要求标记的长度限制在一定范围内。

（2）区分大小写。在标记中必须注意区分大小写。在 HTML 中，标记<HELLO>和<hello>是一回事，但在 XML 中，它们是两个截然不同的标记。

（3）必须有正确的结束标记。结束标记除了要和开始标记在拼写和大小写上完全相同，还必须在前面加上一个斜杠“/”，因此，如果开始标记是<HELLO>，结束标记应该写作</HELLO>。XML 要求标记必须配对出现。不过，为了简便起见，当一对标记之间没有任何文本内容时，可以不写结束标记，而在开始标记的最后以斜杠“/”来确认。这样的标记称为“空标记”，例如：<emptytag/>。

（4）标记间要正确嵌套。在一个 XML 元素中允许包含其他 XML 元素，但这些元素之间必须满足嵌套性，标记不能相互交叉。例如下面是最常见的 HTML 标记重叠的例子，它可以在大多数浏览器中使用，但在 XML 中却是非法的：

```
<B>bold text<I>bold-italic</B>plain italic text…</I>
```

3）属性

标记中可以包含任意多个属性。在标记中，属性以“名称/取值”对的形式出现，属性名不能重复，名称与取值之间用等号“＝”分隔，且取值用引号引起来。例如：

```
<commodity type = "服装" color= "黄色">
```

在这个例子中，type 和 color 是 commodity 标记的属性，“服装”是 type 属性的取值，“黄色”是 color 属性的取值。

属性命名的规范与标记命名规范大体相似，需要注意有效字母、大小写等一系列问题。不过，在必要的时候，属性中也可以包含空格符、标点和实体引用。需要特别注意的是，在 XML 中属性的取值必须用引号引起来，但在 HTML 中这一点并不严格要求。

最后要说明一点，属性的所有赋值都被看作是字符串类型。因此，如果处理程序读到下面这段 XML 标记：

```
<圆柱体 半径="10" 高="13">
```

应用程序应该能够把字符串“10”和“13”转化为它们所代表的数字。

属性和子元素常常能够表述相同的内容，如何判断是使用属性还是子元素有一定难度。一般来说，属性较为简洁、直接，而且有较好的可读性。相反，使用过多的子元素则会使 XML 充斥着大量的开始和结束标记，降低其可读性。在下面几种情况中，宜采用子元素代替属性：

（1）属性不能包含子属性，对于一些复杂的信息，宜采用复合的子元素来说明。

(2) 若元素的开始标记中包含了过多的属性，或标记中的元素名称、属性名称、属性取值过长，造成整个开始标记过长而降低了程序的可读性，则可以考虑使用子元素替代属性。

空格属性和语言属性是XML系统提供的两个特殊属性，使用它们可以说明具体XML元素中的空格和语言特性。

(1) 空格属性的基本形式如下：

空格属性 xml:space

空格属性名为“xml:space”，它用来说明是否需要保留XML元素数据内容中的空格字符。空格属性只有两个可能的取值：default 和 preserve。有些情况下，为了保证XML文档具有较好的可读性，在书写时会引入一些空格和回车符，使用 default 属性值将自动除去这些空格和回车符，还原XML元素内容原有的格式。而使用 preserve 属性值将保留XML元素中的所有空格和回车符。

空格属性是可继承属性，指定一个元素的空格属性后，该元素所包含的所有子元素，除非定义自己的空格属性，否则将继承使用父元素指定的空格属性。

(2) 语言属性的基本形式如下：

语言属性 xml:lang

语言属性用来说明XML元素使用何种语言。语言属性的取值较多，多以国际标准ISO639中编码为标准，如英语的编码是 en，法语的编码为 fr。语言属性的取值也可以使用 IANA (Internet Assigned Numbers Authority)中定义的编码，不过必须增加“I-”或“i-”前缀。用户自定义语言编码则应该以“X-”或“x-”开始。在ISO639编码中，除了说明语种之外，还可以说明区域，例如“en-GB”指英国英语，而“en-US”指美国英语。使用语言属性有助于开发多语种的应用。与空格属性一样，语言属性也是可继承属性。

4) 注释

有时候，希望在XML文件中加入一些用作解释的字符数据，并且希望XML解析器不对它们进行任何处理。这种类型的文本称作注释(comment)文本。

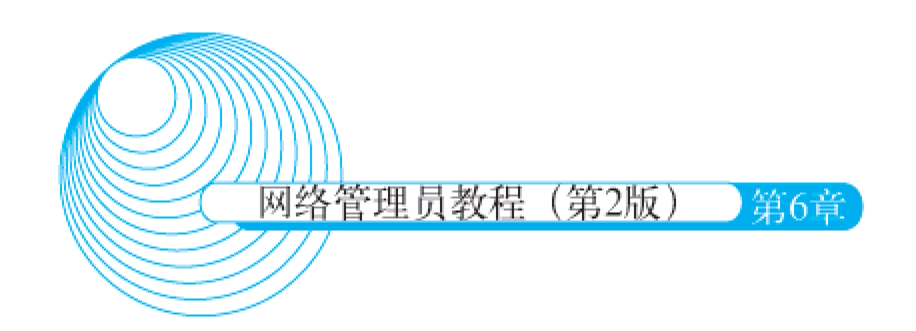
在HTML中，注释是用“＜！ －－”和“－－＞”引起来的。在XML中，注释的方法完全相同，这样看起来会非常亲切。

不过，在XML文件中使用注释时，要遵守以下几个规则。

(1) 在注释文本中不能出现字符“－”或字符串“－－”，XML解析器可能把它们和注释结尾标志“－－＞”相混淆。

(2) 不要把注释放在标记之中。否则，它就不是一个“格式正规”的XML文档。例如下面这段代码：

＜错误注释＜！ －－ 注释文本 －－＞ ＞ ＜/错误注释＞



类似地，不要把注释文本放在实体声明中，也不要放在XML声明之前。记住，永远用XML声明作为XML文件中的第一行。

(3) 注释不能被嵌套。在使用一对注释符号表示注释文本时，要保证其中不再包含另一对注释符号。例如下面例子是不合法的：

```
<! —— 错误 XML 注释嵌套的例子 <! —— 一个注释 ——> ——>
```

使用注释时要确保文件在去掉全部注释之后，遵守所有"格式正规"文档的要求。

5) 内嵌的替代符

字符<、>、&、'和"是XML的保留字符，XML利用它们定义和说明元素、标记或属性等。XML的解析器也将这些字符视为特殊字符，并利用它们来解释XML文档的层次内容结构。这样一来，当XML内容中包含这些字符，并且需要显示它们的时候，就可能会带来混乱和错误。为了解决这个问题，XML使用内嵌的替代符来表示这些系统保留字符。如表6-16所示。

表 6-16 XML 中的内嵌替代符

替代符	含义	例子	解析结果
⁢	<	3⁢5	3<5
>	>	5>3	5>3
&	&	A&B	A&B
'	'	Joe's	Joe's
"	"	"yes"	"yes"

表6-16中"'"和"""只用在属性说明中，在开始标记之外的XML正文中可以直接使用单引号和双引号。

利用内嵌的替代符还可以通过指明字符的Unicode码值来直接说明字符。例如内嵌替代符"&＃163"或"&＃x00A3"代表了码值为163的Unicode字符，即英镑货币符号。

上述的5种内嵌的替代符属于标准的XML实体，是XML实体中最简单的一类，其他复杂的实体将在后面陆续介绍。

6) 处理指令

处理指示(PI，Processing Instruction)用来给处理XML文件的应用程序提供信息。也就是说，XML解析器可能并不处理它，而把这些信息原封不动地传给XML应用程序来解释这个指示并遵照它所提供的信息进行处理。其实，XML声明就是一个处理指示。

所有的处理指示应该遵循下面的格式：

```
<? 处理指示名 处理指示信息? >
```

处理指示名需要服从XML语言的标识符命名规则。定义处理指令，需要把所定义的处理

指令名放在尖括号组成的括号对中，定义处理指令还可以定义若干属性。

由于XML声明的处理指示名是“xml”，因此其他处理指示名不能再用“xml”。例如在本章的例子中，使用一个处理指示来指定与这个XML文件配套使用的样式单的类型及文件名：

```
<? xml-stylesheet type="text/xsl" href="mystyle.xsl"? >
```

处理指令为XML开发人员提供了一种跨越各种元素层次结构的指令表达方式。从而使得应用程序能够按照指令所代表的意义来处理文档。

```
<article>
  <title><? beginUseBold? >节约能源
  </title>
  <content>能源危机<? endUseBold? >早已经不是陌生的话题
  </content>
</article>
```

在上面的文档中，希望将标题和段落的前4个汉字用黑体表示。当然上述效果也可以通过设置元素属性的方式加以处理。

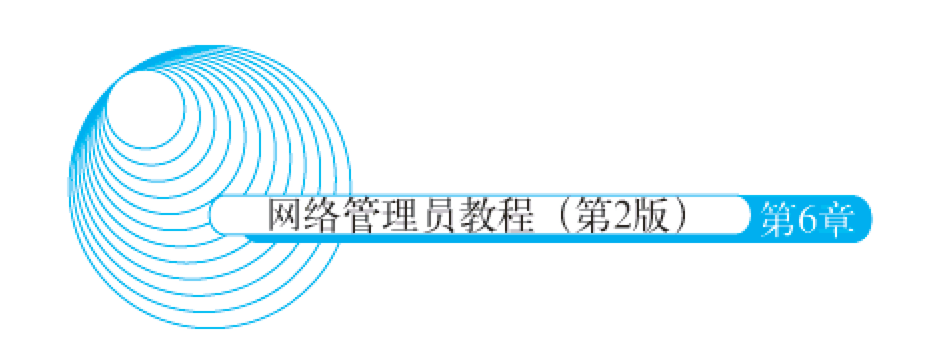
7）CDATA

有些时候，希望XML解析器能够把在字符数据中引入的标记当作普通数据而不是真正的标记来看待。这时，CDATA标记可以助一臂之力。在标记CDATA下，所有的标记、实体引用都被忽略，而被XML处理程序一视同仁地当作字符数据看待。CDATA的基本语法如下：

```
<! [CDATA[文本内容]]>
```

很显然CDATA的文本内容中是不能出现字符串“]]>”的，因为它代表了CDATA数据块的结束标志。前面，讲过XML内嵌的替代符，但是当文本数据中包含大量特殊符号时，不得不通篇地使用替代符，把本来很清晰的一段文字搞得乱七八糟。为了避免这种不便，可以把这些字符数据放在一个CDATA数据块中，这样不管它是否含有元素标签符号和实体引用，这些数据统统被当作没有任何结构意义的普通字符串。例如：

```
<Adress>
    <! [CDATA[
     <联系人>
     <姓名>Jack</姓名>
     <EMAIL>Jack@edu.cn</EMAIL>
     </联系人>
    ]]>
</Adress>
```



只要有字符出现的地方都可以出现 CDATA 部分，但它们不能够嵌套。在 CDATA 部分中唯一能够被识别的字符串就是它的结束分隔符“]]>”。

3．应用程序接口（DOM&SAX）

实际上，XML 文档就是一个文本文件，因此在需要访问文档中的内容时，必须首先书写一个能够识别 XML 文档信息的文本阅读器，也就是通常所说的 XML 解析器（Parser），由它负责对 XML 文档的语法正确性进行验证，并提取其中的内容。XML 文档有时是动态生成的，使得用户能够创建、访问和修改一个 XML 文件。有时候，所开发的应用程序需要能够读懂别人写的 XML 文件，从中提取所需要的信息。

在以上这些情况下，都需要一个类似于 ODBC/JDBC 这样的数据库接口规范的统一的 XML 接口，这个接口使得应用程序与 XML 文档结合在一起，让应用程序能够对 XML 文档提供完全的控制。W3C 意识到了上述问题的存在，于是制订了一套书写 XML 解析器的标准接口规范：文档对象模型（DOM，Document Object Model）。除此之外，XML_DEV 邮件列表中的成员根据应用的需求也自发地定义了一套对 XML 文档进行操作的接口规范—简单应用程序接口（SAX，Simple APIs for XML）。这两种接口规范各有侧重，互有长短，都得到了广泛的应用。

图 6-22 显示了 DOM 和 SAX 在应用程序之间的关系。从图中可以看出，应用程序不是直接对 XML 文档进行操作的，而是首先由 XML 解析器对 XML 文档进行分析，然后，应用程序通过 XML 分析器所提供的 DOM 接口或 SAX 接口对分析结果进行操作，从而实现了对 XML 文档的访问。

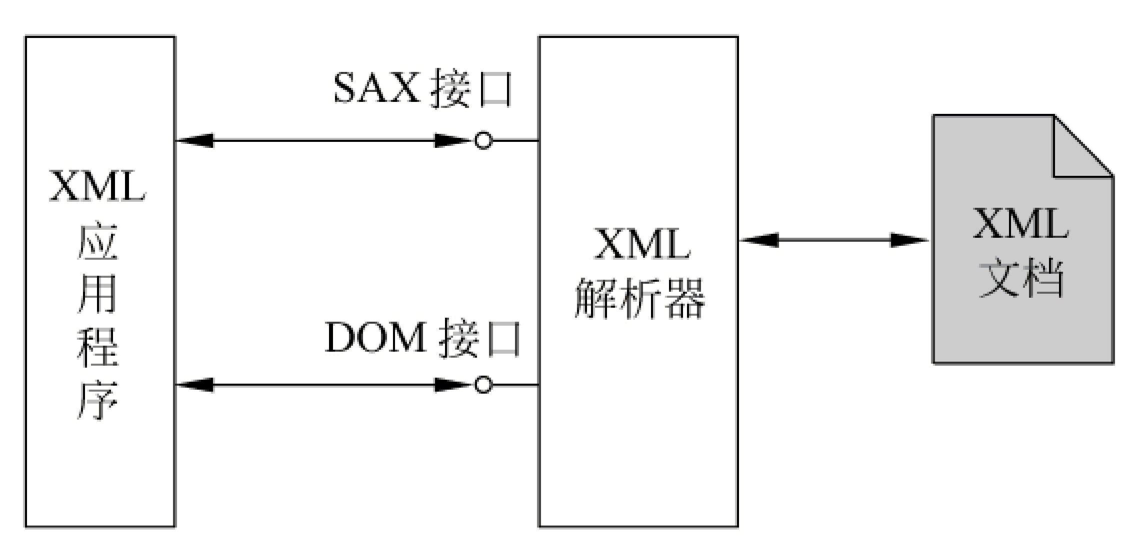


图 6-22　XML 程序接口示意

1）文档对象模型（DOM）

DOM 的全称是文档对象模型（Document Object Model）。在应用程序中，基于 DOM 的 XML 解析器将一个 XML 文档转换成一棵 DOM 树，应用程序正是通过 DOM 树来实现对 XML 文档数据的操作。通过 DOM 接口，应用程序可以在任何时候访问 XML 文档中的任何一部分数据，因此，这种利用 DOM 接口的机制也被称作随机访问机制。

无论 XML 文档中所描述的是什么类型的信息，利用 DOM 所生成的模型都是节点树的形

式。也就是说，DOM强制使用树模型来访问XML文档中的信息。在这种模型下，每个元素对应一个节点，而每个节点都可以包含它自己的节点子树，在每个文档的顶端是文档根节点。由于XML本质上就是一种分层结构，所以这种描述方法是相当有效的。

```
<? xml version="1.0"? >

<address>
  <person sex = "male">
    <name>Jack</name>
    <email>Jack@xml.net </email>
  </person>

  <person sex = "male">
    <name>John</name>
    <email>john@xml.net</email>
  </person>
</address>
```

用DOM来表示这段文档，如图6-23所示。

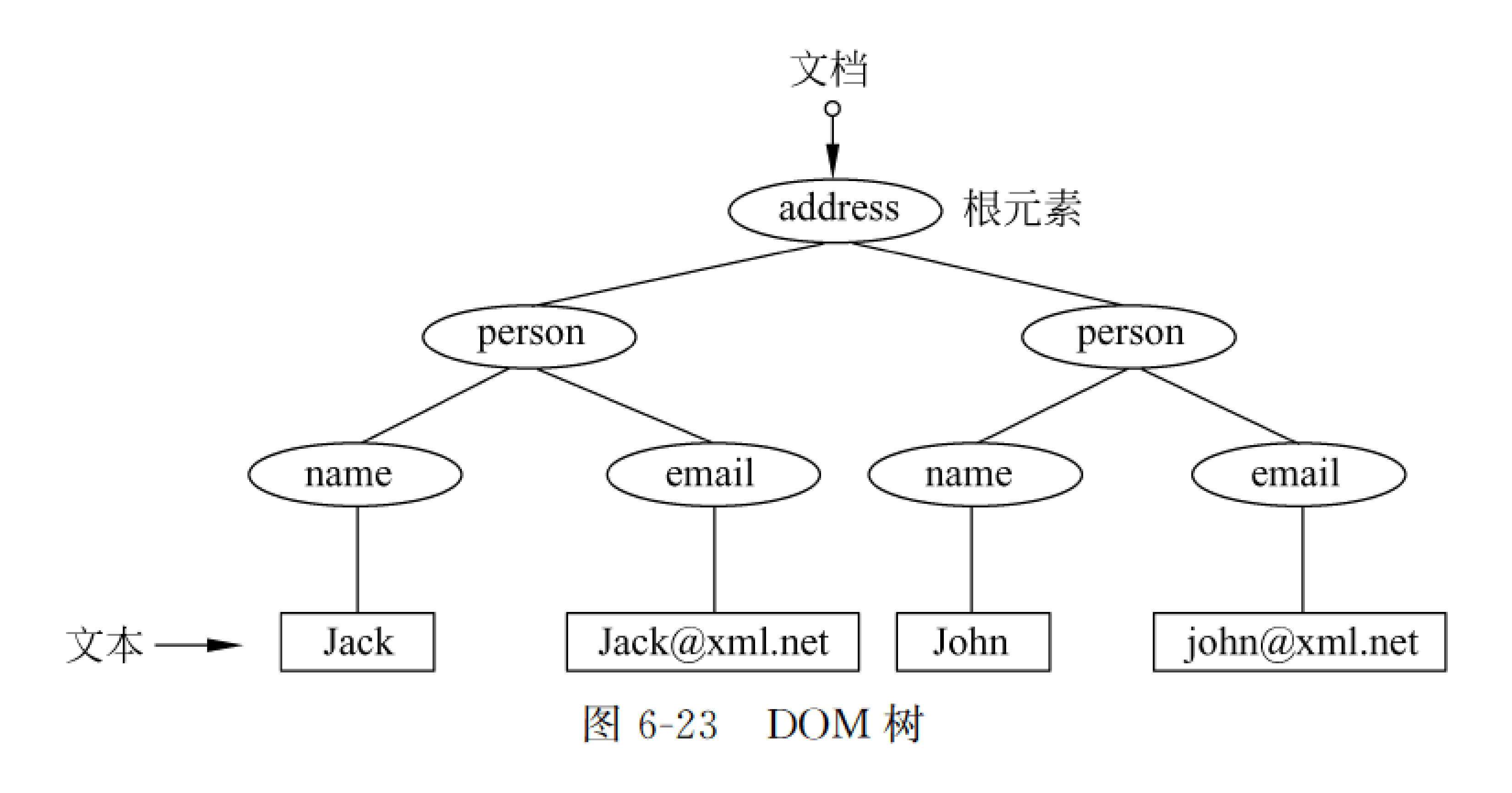
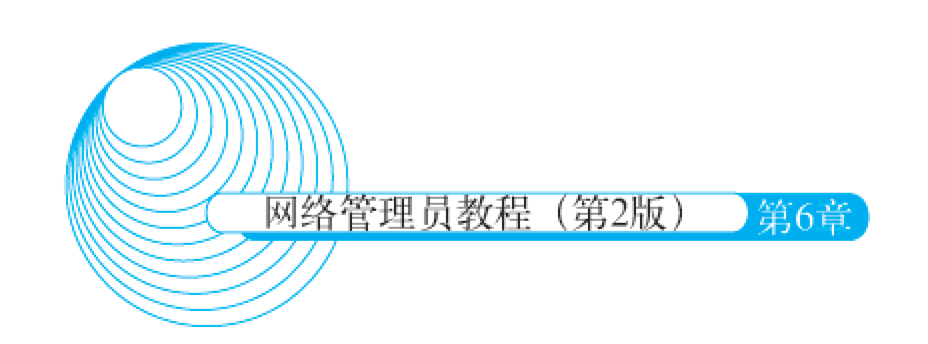


图6-23 DOM树

应用程序通过对该对象模型的操作，实现对XML文档中数据的操作。DOM API提供给用户的是一种随机访问机制。通过它，应用程序不仅可以在任意时候访问XML文档中的任何数据，而且可以任意地插入、删除、修改、移动和存储XML文档中的内容。它提供了一种访问操作存储在XML文档内信息的标准化方法，搭建了应用程序和XML文档之间联系的桥梁。

由于DOM解析器把整个XML文档转化成DOM树放在了内存中，因此，当文档比较大或者结构比较复杂时，对内存的需求就比较高。而且，对于结构复杂的树的遍历也是一项耗时的



操作。所以，DOM 解析器对机器性能的要求比较高，实现效率不十分理想。不过，由于 DOM 解析器所采用的树结构的思想与 XML 文档的结构相吻合，同时鉴于随机访问所带来的方便，因此，DOM 解析器的应用十分广泛。

2）简单应用程序接口（SAX）

SAX 的全称是 XML 简单应用程序接口（Simple APIs for XML）。与 DOM 不同，SAX 采用顺序访问模式，是一种快速读写 XML 数据的方式。当使用 SAX 解析器对 XML 文档进行分析时，会触发一系列事件，并激活相应的事件处理函数，应用程序通过这些事件处理函数实现对 XML 文档的访问，因而 SAX 接口也被称作事件驱动接口。

SAX 提供的是一种顺序访问机制，对于已经解析过的部分，不能再倒回去重新处理。SAX 之所以被叫做“简单”应用程序接口，是因为 SAX 解析器只做了一些简单的工作，大部分工作还要由应用程序自己去做。也就是说，SAX 解析器在实现时，它只是顺序地检查 XML 文档中的字节流，判断当前字节是 XML 语法中的哪一部分、是否符合 XML 语法，然后再触发相应的事件，而事件处理函数本身则要由应用程序自己来实现。同 DOM 分析器相比，SAX 解析器缺乏灵活性。然而，由于 SAX 解析器实现简单，对内存要求比较低，因此实现效率比较高，对于那些只须访问 XML 文档中的数据而不对文档进行更改的应用程序来说，SAX 解析器更为合适。

SAX 解析器的大体构成框架如图 6-24 所示。图 6-24 中最上方的 SAXParserFactory 用来生成一个分析器实例。XML 文档是从左侧箭头所示处读入，当解析器对文档进行分析时，就会触发在 DocumentHandler，ErrorHandler，DTDHandler 以及 EntityResolver 接口中定义的回调方法。

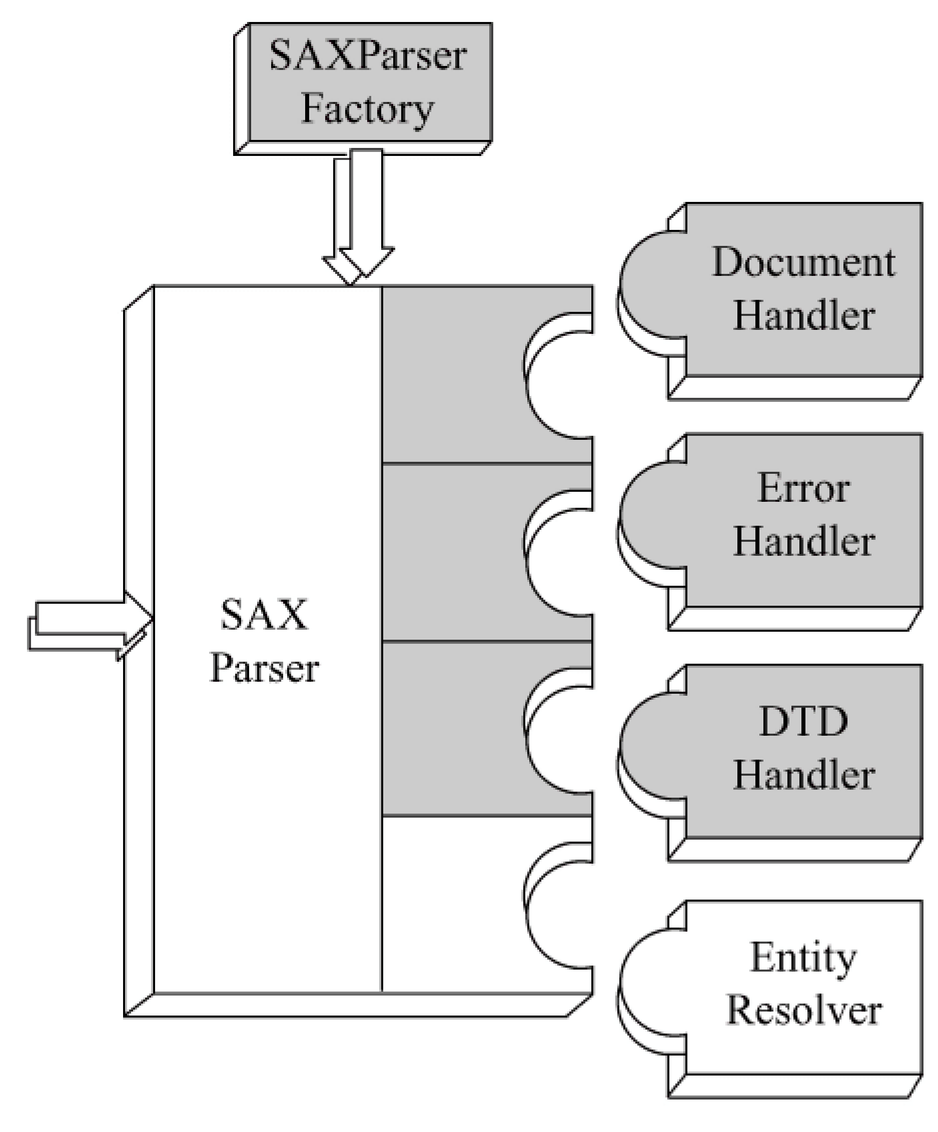


图 6-24　SAX 解析器的结构

4. XML 文档的显示

HTML 中的标记主要用来说明 HTML 文档在浏览器中的显示格式，所以 HTML 文档的显示格式基本是固定的。而 XML 中的标记是开发者定义的，主要用来说明 XML 程序文档所表述的数据的内在结构关系。这样一来，XML 程序文档的显示格式就需要用另外的机制来定义。层叠样式单（CSS，Cascading Style Sheet）和扩展样式单语言（XSL，eXtensible Style Sheet Language）是 W3C 推荐的表达 XML 文档数据显示格式的两种标准。

1）层叠样式单（CSS）

层叠样式单最早是为方便 HTML 语言而提出的，使用层叠样式单能保证文档显示格式的一致性和较好的格式化，在 XML 中使用层叠样式单可以方便开发人员为自定义的元素和标记定义其显示格式。通过层叠样式单可以产生上百种显示格式信息，例如字体，颜色，位置等。

层叠样式单信息可以以属性、属性组或独立文件的形式存在。一般认为以独立文件的形式存在较好，因为这样可以方便层叠样式单信息的管理、修改、维护和复用。

层叠样式单的功能虽不如扩展样式单语言强，但其实际和开发过程相对容易的多。在此不详细介绍 CSS 标准，需要了解这一技术细节可以参考其他书籍。

2）扩展样式单语言（XSL）

CSS 是一种静态的样式描述格式，其本身不遵从 XML 的语法规范。扩展样式单语言不同，它遵守 XML 的语法规则，是 XML 的一种具体应用。这也就是说，XSL 本身就是一个 XML 文档，系统可以使用同一个 XML 解释器对 XML 文档及其相关的 XSL 文档进行解释处理。

XSL 语言可分为 3 个不同的部分：

- 转换工具（XSLT，XSL Transformations）。它描述了如何将一个没有形式表现的 XML 文档内容转换为可浏览或可输出的格式。
- 格式对象（FO，Formatted Object）。
- XML 分级命令处理工具 XPath。

一个 XML 文档的显示过程是这样的：首先根据 XML 文档构造源树；然后根据给定的 XSL 将这个源树转换为可以显示的结果树，这个过程称作树转换；最后再按照 FO 解释结果树，产生一个可以在屏幕上、纸上、语音设备或其他媒体中输出的结果，这个过程称作格式化。

描述树转换的这一部分协议日趋成熟，已从 XSL 中分离出来，另取名为 XSLT，其正式推荐标准于 1999 年 11 月 16 日公布，现在一般所说的 XSL 大都指的是 XSLT。与 XSLT 一同推出的还有其配套标准 XPath，这个标准用来描述如何识别、选择、匹配 XML 文档中的各个构成元件，包括元素、属性、文字内容等。

XSLT 主要的功能就是转换，它将一个 XML 文档作为一个源树，将其转换为一个有样式信息的结果树。在 XSLT 文档中定义了与 XML 文档中各个逻辑成分相匹配的模板，以及匹配转换方式。值得一提的是，尽管制订 XSLT 规范的初衷只是利用它来进行 XML 文档与可格式化对象之间的转换，但它的巨大潜力却表现在它可以很好地描述 XML 文档向任何一个其他格式的文档作转换的方法，例如转换为另一个逻辑结构的 XML 文档、HTML 文档、XHTML 文档、VRML 文档、SVG 文档等，不一而足。限于目前浏览器的支持能力，大多数情况下是转换为一个 HTML 文档进行显示。

具体的转换过程，既可以在服务器端进行，也可以在客户端进行。两者分别对应着不同的转换模式：

- 服务器端转换模式。在这种模式下，XML 文件下载到浏览器前先转换成 HTML，然后

再将 HTML 文件送往客户端进行浏览。

- 客户端转换模式。这种方式是将 XML 和 XSL 文件都传送到客户端，由浏览器实时转换。前提是浏览器必须支持 XML+XSL。

下面来看一个 XSLT 的简单例子。通过剖析这个例子，可以对 XSLT 的基本语法和功能有一个了解。

```
<? xml version="1.0" encoding="gb2312" ? >
<? xml-stylesheet type="text/xsl" href="mystyle.xsl"? >
<roster>
    学生花名册
    <student>
      <name>李华</name>
      <origin>河北</origin>
      <age>15</age>
      <telephone>62875555</telephone>
    </student>
      <student>
      <name>张三</name>
      <origin>北京</origin>
      <age>14</age>
      <telephone>82873425</telephone>
    </student>
</roster>
```

```
<? xml version="1.0" encoding="gb2312" ? >
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns="http://www.w3.org/TR/REC-html40">
<xsl:template>
<xsl:apply-templates/>
</xsl:template>

<xsl:template match="/">
<HTML>
   <HEAD>
     <TITLE>学生花名册</TITLE>
    <STYLE> .title{font-size:15pt; font-weight:bold; color:blue } .name{color:red}
    </STYLE>
```

```
      </HEAD>
      <BODY>
        <P class="title" >学生花名册</P>
        <xsl:apply-templates select="roster"/>
    </BODY>
      </HTML>
    </xsl:template>

    <xsl:template match="roster">
    <TABLE BORDER="1">
        <THEAD>
          <TD> <B>姓名</B> </TD>
          <TD> <B>籍贯</B> </TD>
          <TD> <B>年龄</B> </TD>
          <TD> <B>电话</B> </TD>
        </THEAD>
        <xsl:for-each select="student" order-by="name">
        <TR>
          <TD><B><xsl:value-of select="name"/></B></TD>
          <TD><xsl:value-of select="origin"/></TD>
          <TD><xsl:value-of select="age"/></TD>
          <TD><xsl:value-of select = "telephone"/></TD>
        </TR>
        </xsl:for-each>
      </TABLE>
    </xsl:template>
    </xsl:stylesheet>
```

可以看出，在 XML 中声明 XSL 样式单的格式是：

```
<? xml-stylesheet type="text/xsl" href="样式单文件名"? >
```

为看懂上例中的 XSL 源码，首先介绍一下 XSL 的几条主要语句。

（1）xsl:stylesheet：声明语句。

（2）xsl:template：相当于编程中函数的概念。

（3）xsl:template match = ""：相当于函数调用，去匹配引号中指定的节点。

（4）xsl:apply-templates：应用模板函数。

（5）xsl:apply-templates select =""：应用模板函数的调用，跳转到引号中指定的模板。

（6）xsl:for-each select ＝ ""：循环语句，遍历与引号中的属性值相同的节点。

（7）xsl:value-of select ＝ ""：赋值语句，取出引号中指定的属性值。

知道了上面这些语句的含义，就可以分析一下这段 XSLT 源代码的执行过程了，整个过程如图 6-25 所示。在 IE 中的浏览效果如图 6-26 所示。

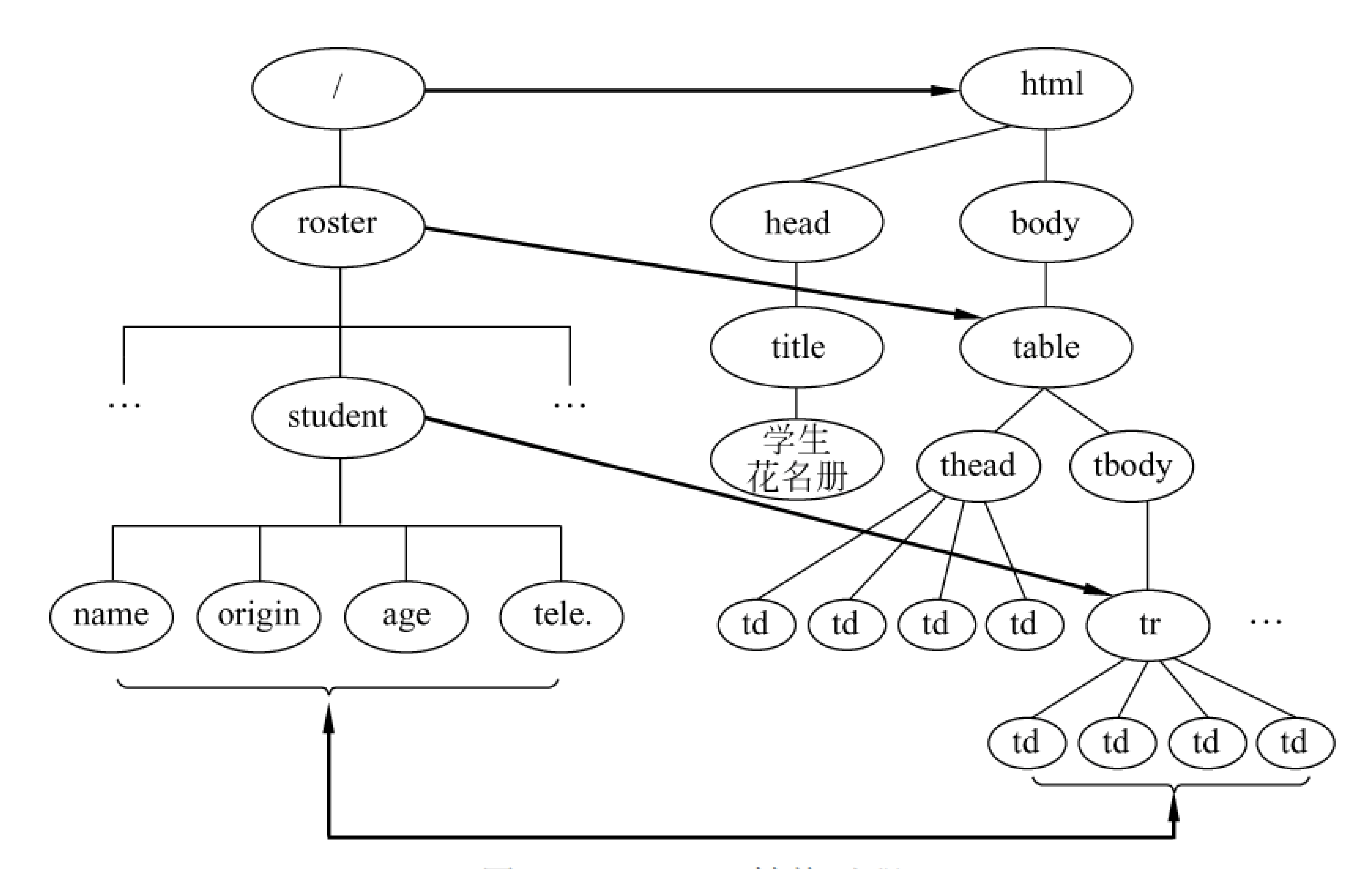
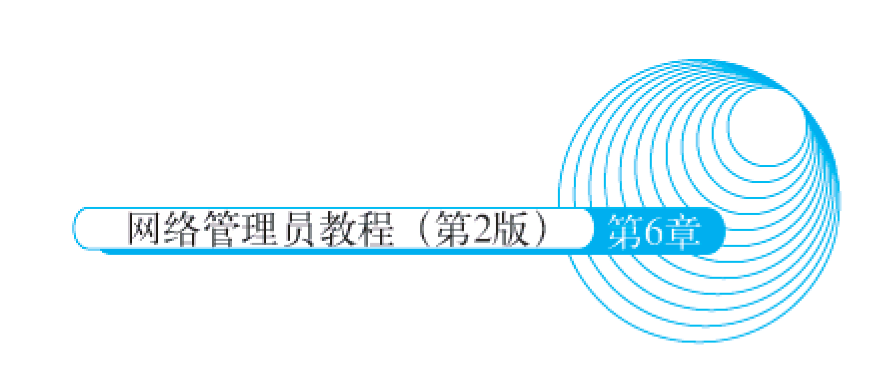


图 6-25　XSLT 转换过程



姓名	籍贯	年龄	电话
李华	河北	15	62875555
张三	北京	14	82873425

图 6-26　XML 文档在 IE 中的显示



6.4 Web 网站创建与维护

6.4.1 Web 网站的创建

1. 组织信息

在创建网站之前,必须考虑如下问题:

(1) 信息如何被分解成一系列有组织的主题。

(2) 一个网站需要多少个网页链接在一起才能完成必须要讲述的内容,每个网页需要多大容量。

(3) 粗略记录信息将会覆盖的主题或子主题的一个列表。计算有多少个这样的主题,每一个主题需要多少内容,这样才能够对文档的规模和范畴有一个比较恰当的理解。

(4) 查看这些主题是否按照从开始到结束的逻辑顺序进行,其中每一个新的部分是否取决于前面部分的内容。或者,这些材料看上去是否很自然地分解成了一些子主题(以及更低级别的主题),如何调整主题的次序,才使得它们之间的过渡更符合逻辑,或者将相关主题组织在一起。

2. 构建网站框架

在编写文档之前,对框架做越多的优化,就会越紧扣主题,而且编码的效率也会越高。更重要的是,最后所产生的 Web 文档将以一种清晰而明朗的方式来展现信息。

在构建框架时,需要考虑的是展示的逻辑组织以及它的内容,它们如何才能够和网页上能够看到的一些通常的组织结构相匹配,以下是几种逻辑组织。

(1) 布告板:一个单独的、简单的网页,它通常描述一个人、小的业务或者简单的产品。大多数的个人网站都是这种类型。它们通常包含一些链接,这些链接是指向网络上的相关资源的,但是不指向相同文档内的任何其他网页。

(2) 单页线性:一个网页,或长或短,它被设计成从头到尾地进行阅读。通常使用一些规则将这样一个网页分解成虚拟的“页”。读者可以翻阅整个网页,但是也可以使用内容和目标的表格来快速跳至任何部分。这种类型最适合于比较短的文档(少于 10 个满屏),而且这个文档中所有的信息很自然地从头到尾过渡。

(3) 多页线性:和单页线性的基本思想相同,但是它被分解成多个逻辑上连贯的、一个接一个的网页,从开头到结束,就像一个故事一样。通过放置在每一页底部的一个指向下一页的链接来引导读者遍历整个系列的网页。

(4) 分层:典型的网站结构。一个首页(有时候会与主页混淆)包含到其他网页的链接,每

一页包含一个主要的主题区。每一个这样的网页又可以包含指向更多网页的多个链接，进一步将主题分解。这样的结果便是一个树型的结构，如图 6-27 所显示。

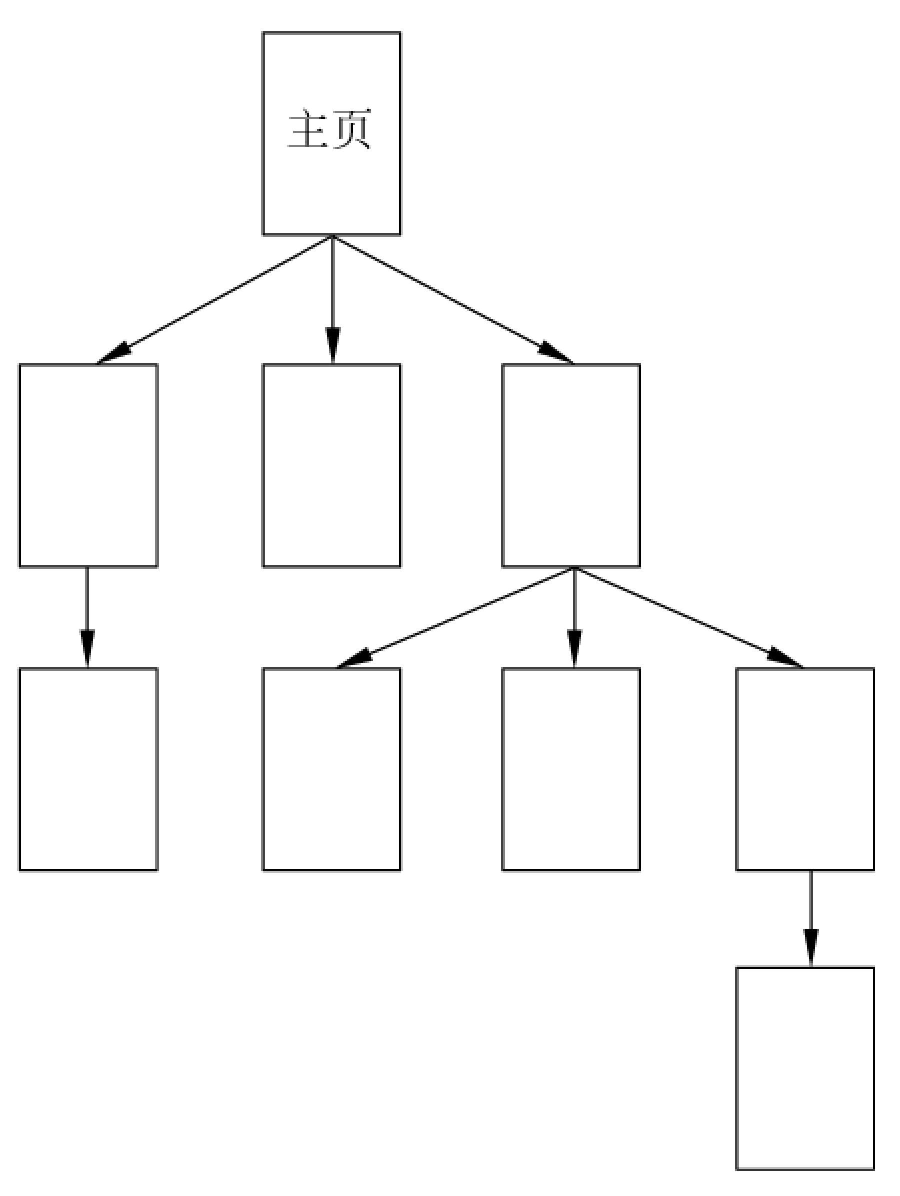


图 6-27　分层网站结构

（5）网状：一个网状的结构是一个没有层次的分级的结构，如图 6-28 所示。这样的文档中有多个网页，而在其中的任意一个网页又都包含有连接到其他网页的链接。可能会有一个首页，但是从那里进入之后，读者就可以在此网中逛来逛去，且不须沿一个特定的路径。网状的结构是松散并且自由游走的，最适宜于娱乐、休闲的主题，或者那些难于进行顺序或层次分解的主题。

3. 建立 Web 服务器

Web 服务器是用来存储网页并响应执行用户的访问请求的设备。Web 服务器可以提供多种服务，这些服务包括打印、数据库、WWW、FTP、电子邮件、文件管理等。Web 服务器是一种网络服务器，运行另外的软件以提供 WWW 服务。Web 服务器对通过因特网使用 HTTP 协议的文件、文件夹以及其他资源的访问进行管理。当前两种最流行的 Web 服务器是运行于 Linux 操作系统平台之上 Apache Web 服务器和运行于 Windows 操作系统平台之上的 Microsoft 的 IIS Web 服务器。

Web 服务器要处理执行程序、追踪目录和文件，并且还要与计算机进行各种通信。用户会请求 Web 服务器执行一些操作，也会对 Web 服务器上的文件发出请求。另外，可以使用某些技

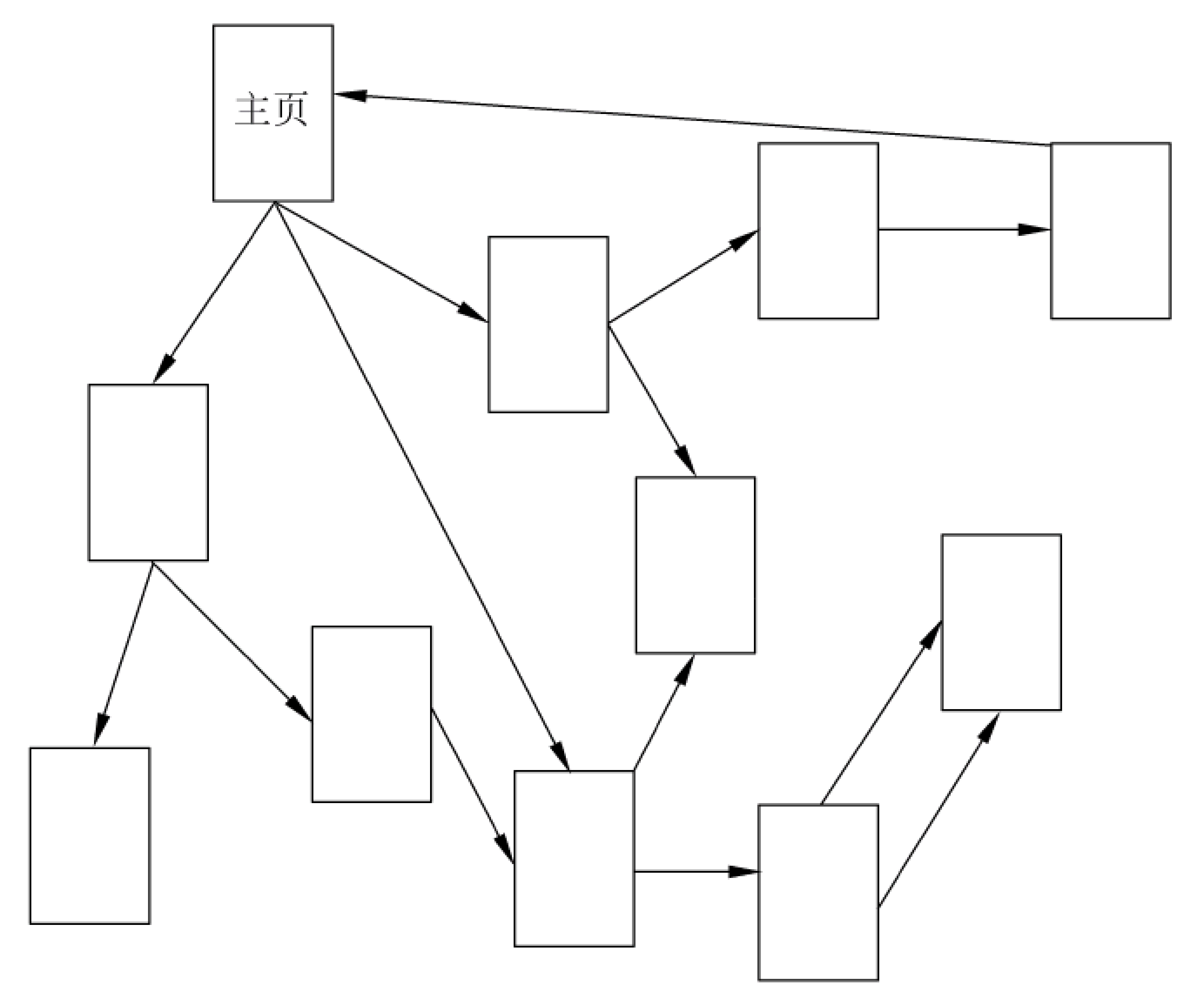


图 6-28　网状网站结构

术来增强 Web 服务器的功能，使其除了提交标准的 HTML 页面之外还有其他的功能，这些技术包括 CGI 脚本、SSL 协议、Java 小程序、动态服务器页等。Web 服务器利用硬盘空间来发布 Web 网页。

获得 Web 服务器空间有几种方式：

(1) 企业或单位内部的已建 Web 服务器；

(2) 托管 Web 主机，越来越多的在线公司提供 Web 空间“托管服务”；

(3) 新建 Web 服务器。如果网页需要非常严格的安全性或者需要大量使用脚本(尤其是表单)，通常需要新建一个 Web 服务器。

企业或单位安置服务器需要下列的硬件、软件，还需要相关人员来架设并维护 Web 服务器。

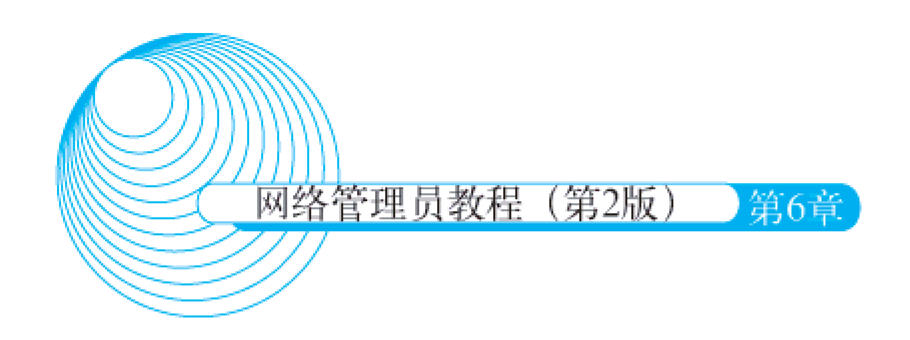
(1) 服务器硬件。

(2) Web 服务器软件。常用的有以下几种：

- 在 Windows NT 和 Windows 2000 Sever 上运行的 Microsoft Internet Information Server (IIS)。
- Apache Web Server。
- 可跨平台使用的 Netscape 和 Sun Microsystems 的 iPlanet Web Server。
- 在 Novell NetWare 上运行的 Netscape Enterprise Server。

(3) 可提供 24 小时访问服务的因特网连接。

(4) 用来将本地网与 Web 网络通信隔开的路由器。



(5) 用来保护系统安全的防火墙。

(6) 后备电源。

(7) 保证服务器全天候正常运行的计划。

(8) 管理系统操作并负责维护工作的 Web 服务器管理员。

4. 域名注册

每台 Web 服务器都需要域名解析服务器将它的域名转换成 IP 地址。在进行域名选择之前，首先要权衡需求。考虑域名需要拥有什么样的含义，例如是否需要包含商标名、产品类型，以及是否要将 URL 印制出来进行宣传等。注册的域名最好引人瞩目而过目难忘。如果公司已拥有公认的商标或者名字，就可以用它们来做域名。域名将成为企业在网络上的品牌，所以选择一定要谨慎，不能有歧义。

域名选好后，就可以到中国互联网络信息中心(www.cnnic.net.cn)进行注册了。注册域名时，可以通过联机注册、电子邮件等方式向域名注册服务机构递交域名注册申请表，提出域名注册申请，并且与域名注册服务机构签订域名注册协议。

5. Web 网站的发布

在发布之前，需要准备和了解一些关于 Web 服务器的相关信息。

(1) 用于上载文件所使用协议的名字。很多服务器允许使用 Web 协议(HTTP)来上载文件，而有些则要求通过 FTP 来上载文件。

(2) 要记录文件将要存储的目录的完整的 URL，这包括从服务器的名字，一直到文件的所在目录的路径。

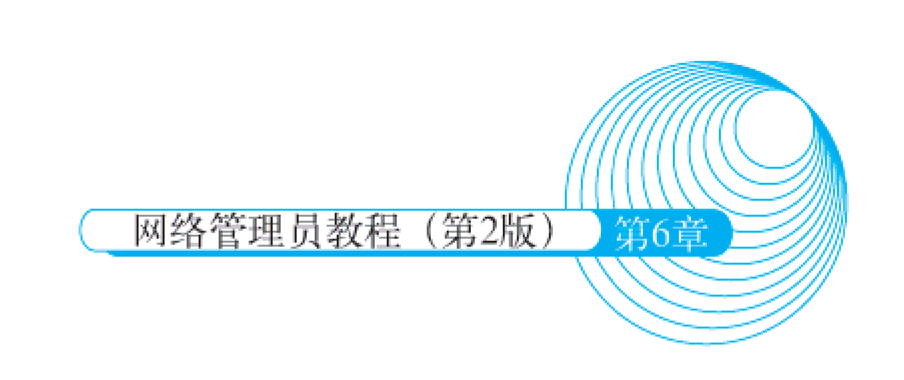
(3) 服务器上文件名的规则和限制。

(4) 用于上载访问此服务器的唯一的用户名和口令。

将文件发布到 Web 服务器，可通过 FTP 工具软件，将文件从本地计算机传输到远程 Web 服务器上去。在文件传输到 Web 服务器上之后，要对站点进行测试。如要使用的 Web 服务器与开发时使用的 Web 服务器属于不同的类型，测试就格外重要。如果是要替换旧网站，把站点上传到 Web 服务器后，就要暂时将服务器离线。或在访问服务器的用户很少时上传文件，同时要预先通知用户，服务器会停机一段时间。

6.4.2 Web 网站的维护

当网页在线之后，很重要的问题是了解如何来更新以及如何来测试它，这样就可以让它保持向访问者可靠地开放。



1. 网站维护

1）网站更新

Web发布后，可对其内容进行持续更新。Web发布永远都没有最终版本。修改时，只须修订一个版本（即服务器上的版本）即可。简单的修改可以在几分钟之内完成，且用户马上就能浏览。修改不必局限于对已有功能的细化，也可根据需求增加新的功能，还可以随着业务的增长和新产品的上市而增加新的内容，甚至可以加入一些实时变更的内容。这些修改对于网站特色是非常重要的。诸如在线杂志之类的Web刊物就需要经常更新其外观和内容，以保持对用户的吸引力。在规划网站时，不能忽视网站持续修改和更新的能力。Web用户希望网站内容及时并且经常更新，因此必须准备好根据客户和客户的产品来提供最新信息的公告。尽早获取要发布信息的内容和副本，并做成HTML，然后在合适的时间发布。

2）给内容加上日期标注

对于一个以内容为主的网站而言，用户判断哪些是最新内容可能会有些困难。为了避免这种情况发生，可以给网上内容加上日期标注，指出该信息的发布时间和删除时间，可以指出哪些是陈旧的内容，从而有助于网站维护。删除过期内容要小心，因为有人可能将该页标记为书签。如有人根据书签进入被删除页，就会报错。所以最好不要删除页面，而改用新内容来更新这些页面。

3）设计的修改

修改是不可避免的，为了使修改变得容易，应预先设计好修改时要用到的规格说明和模板。这些文档是在设计过程的开始阶段创建的，文档中要确定字体、字号、颜色、背景图像等元素。

4）规划更新内容

内容更新要有一个规划，否则容易导致网站内容过期。可定期使用以下方案来确保网站的更新：

（1）单击所有链接。替换或删除损坏的链接。

（2）确保目前使用的是最新版本的文件。

（3）让客户浏览网站，找出过期内容。

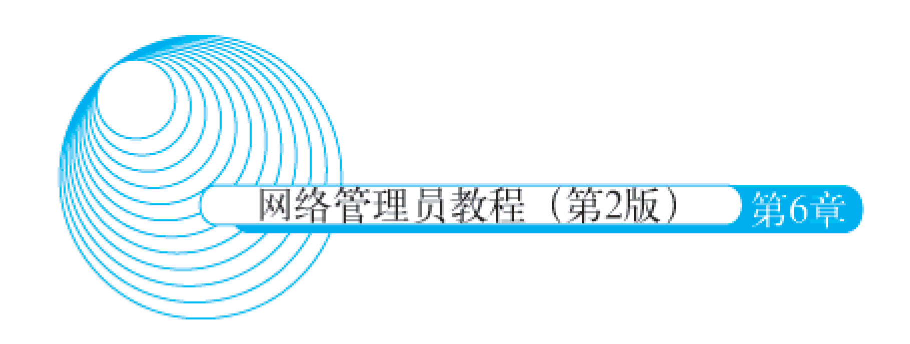
（4）查看是否有重要信息发生变化，如电话号码、产品价格等。

5）跟踪网站行为

可以跟踪网站行为，例如网站的访问次数，用户进入网站的途径，以及用户浏览网站的方式。可以使用这些信息来检查网站的导航设计方案、网站广告以及与其他网站的链接。

6）用户支持

任何时候都应为用户提供某种形式的在线用户支持。可以考虑加入到网站中的用户支持功能包括：反馈途径，FAQ页面，甚至包括复杂的数据库驱动搜索引擎。



2. 网站测试

1）测试浏览器的可变性

网页用(IE,Internet Explorer)来查看时的外观和功能是好的。但是使用 Netscape 浏览器的用户就可能会遇到一些问题。不同的浏览器会呈现出显著的区别。

要确保网页的外观对于所有人浏览器都是可以接收的,需要在线地用不同种类的浏览器来查看网页。在线浏览 Web 的人们,绝大多数是通过 IE 或者 Netscape Navigator 来浏览的,通常需要测试这两个最大的浏览器的最新版本。另外,在当前的 IE 或者 Navigator 版本中测试没有问题的网页,可能在使用一个一两年前的浏览器来查看时可能会出现一些问题。通常要保留 IE 或者 Navigator 等的旧版本,用于测试网页。

2）测试不同的分辨率

评价网页时,需要在不同的分辨率下进行测试。要这样做,就必须在 Windows 中改变显示分辨率,然后再查看此网页。在改变了分辨率之后,再打开浏览器,可能会发现浏览器的窗口不再是完全最大化的"满屏"大小,或者最大化之后页面内容不居中,这些都是要解决的问题。

3）测试链接的有效性

最后,很重要的一点是测试网页中的所有链接。一是要测试内部链接(本网站的文件之间的链接)。每次对网站做了变动之后,都要重新测试这些链接。二是要测试指向外部的链接(不在本网站服务器上的链接)。要经常检查这些链接,至少一个月检查一次所有的外部链接。

第7章　网络安全

7.1　网络安全基础

7.1.1　网络安全基本概念

由于计算机网络的迅猛发展，网络安全已成为网络发展中的一个重要课题。由于网络传播信息快捷，隐蔽性强，在网络上难以识别用户的真实身份，网络犯罪、黑客攻击、有害信息传播等方面的问题日趋严重。网络安全的产生和发展，标志着传统的通信保密时代过渡到了信息安全时代。

1. 网络安全基本要素

网络安全包括5个基本要素：机密性、完整性、可用性、可控性与可审查性。

(1) 机密性：确保信息不暴露给未授权的实体或进程。

(2) 完整性：只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改。

(3) 可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。

(4) 可控性：可以控制授权范围内的信息流向及行为方式。

(5) 可审查性：对出现的网络安全问题提供调查的依据和手段。

2. 网络安全威胁

一般认为，目前网络存在的威胁主要表现在以下方面。

(1) 非授权访问：没有预先经过同意，就使用网络或计算机资源则被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

(2) 信息泄漏或丢失：指敏感数据在有意或无意中被泄漏出去或丢失，它通常包括：信息在传输中丢失或泄漏、信息在存储介质中丢失或泄漏以及通过建立隐蔽隧道等窃取敏感信息等。如黑客利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推测出有用信息，如用户口令、账号等重要信息。

(3) 破坏数据完整性：以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

（4）拒绝服务攻击：它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

（5）利用网络传播病毒：通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

（6）混合威胁攻击：混合威胁是新型的安全攻击，主要表现为一种病毒与黑客程序相结合的新型蠕虫病毒，可以借助多种途径和技术潜入企业、政府、银行、军队等的网络。这些利用“缓存溢出”对其他网络服务器进行传播的蠕虫病毒，还具有持续发作的特点。混合威胁的出现说明病毒编写者正在利用大量的系统漏洞将病毒传播的速度最大化。

（7）间谍软件、广告程序和垃圾邮件攻击：近年在全球范围内最流行的攻击方式是钓鱼式攻击，它利用间谍软件、广告程序和垃圾邮件将用户引入恶意网站，这些网站看起来与正常网站没有什么两样，但犯罪分子通常会以升级账户信息为由要求用户提供机密资料。

3. 网络安全控制技术

为了保护网络信息的安全可靠，除了运用法律和管理手段外，还需依靠技术方法来实现。网络安全控制技术目前有：防火墙技术、加密技术、用户识别技术、访问控制技术、网络反病毒技术、网络安全漏洞扫描技术、入侵检测技术、统一威胁安全管理技术等。

（1）防火墙技术。防火墙技术是近年来维护网络安全最重要的手段。根据网络信息保密程度，实施不同的安全策略和多级保护模式。加强防火墙的使用，可以经济、有效地保证网络安全。目前已有不同功能的多种防火墙。但防火墙也不是万能的，需要配合其他安全措施来协同防范。

（2）加密技术。加密技术是网络信息安全主动的、开放型的防范手段，对于敏感数据应采用加密处理，并且在数据传输时采用加密传输，目前加密技术主要有两大类：一类是基于对称密钥的加密算法，也称私钥算法；另一类是基于非对称密钥的加密算法，也称公钥算法。加密手段，一般分软件加密和硬件加密两种。软件加密成本低而且实用灵活，更换也方便，硬件加密效率高，本身安全性高。密钥管理包括密钥产生、分发、更换等，是数据保密的重要一环。

（3）用户识别技术。用户识别和验证也是一种基本的安全技术。其核心是识别访问者是否属于系统的合法用户，目的是防止非法用户进入系统。目前一般采用基于对称密钥加密或公开密钥加密的方法，采用高强度的密码技术来进行身份认证。比较著名的有 Kerberos、PGP 等方法。

（4）访问控制技术。访问控制是控制不同用户对信息资源的访问权限。根据安全策略，对信息资源进行集中管理，对资源的控制粒度有粗粒度和细粒度两种，可控制到文件、Web 的 HTML 页面、图形、CCT、Java 应用。

(5) 网络反病毒技术。计算机病毒从1981年首次被发现以来，在近20年的发展过程中，在数目和危害性上都在飞速发展。因此，计算机病毒问题越来越受到计算机用户和计算机反病毒专家的重视，并且开发出了许多防病毒的产品。

(6) 漏洞扫描技术。漏洞检测和安全风险评估技术，可预知主体受攻击的可能性和具体地指证将要发生的行为和产生的后果。该技术的应用可以帮助分析资源被攻击的可能指数，了解支撑系统本身的脆弱性，评估所有存在的安全风险。网络漏洞扫描技术，主要包括网络模拟攻击、漏洞检测、报告服务进程、提取对象信息以及评测风险、提供安全建议和改进措施等功能，帮助用户控制可能发生的安全事件，最大可能地消除安全隐患。

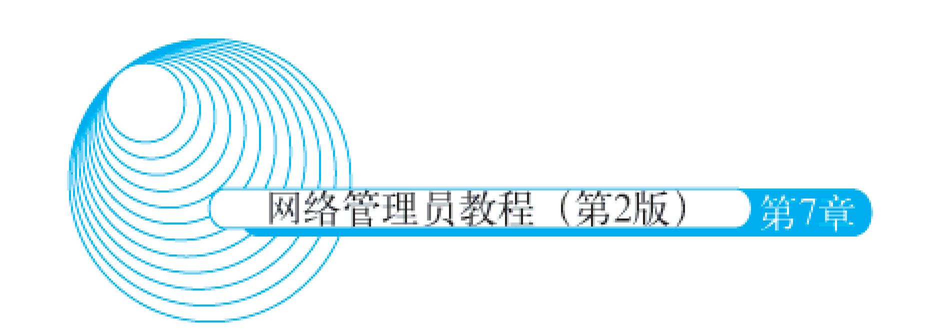
(7) 入侵检测技术。入侵行为主要是指对系统资源的非授权使用。它可以造成系统数据的丢失和破坏，可以造成系统拒绝合法用户的服务等危害。入侵者可以是一个手工发出命令的人，也可以是一个基于入侵脚本或程序的自动发布命令的计算机。入侵者分为两类：外部入侵者和允许访问系统资源但又有所限制的内部入侵者。内部入侵者又可分成：假扮成其他有权访问敏感数据用户的入侵者和能够关闭系统审计控制的入侵者。入侵检测是一种增强系统安全的有效技术。其目的就是检测出系统中违背系统安全性规则或者威胁到系统安全的活动。检测时，通过对系统中用户行为或系统行为的可疑程度进行评估，并根据评估结果来鉴别系统中行为的正常性，从而帮助系统管理员进行安全管理或对系统所受到的攻击采取相应的对策。

(8) 统一威胁安全管理技术。统一威胁安全管理技术（UTM）是保持威胁生态平衡的一种方法，由硬件、软件和网络技术组成的具有专门用途的设备，它主要提供一项或多项安全功能。它将多种安全特性集成于一个硬设备里，构成一个标准的统一管理平台，UTM设备应该具备的基本功能包括网络防火墙、网络入侵检测/防御和网关防病毒功能，该项技术需要一定的技术过渡期。

7.1.2 黑客的攻击手段

涉及网络安全的问题很多，但最主要的问题还是人为攻击，黑客就是最具有代表性的一类群体。黑客的出现可以说是当今信息社会，尤其是在因特网互联全球的过程中，网络用户有目共睹、不容忽视的一个独特现象。黑客在世界各地四处出击，寻找机会袭击网络，几乎到了无孔不入的地步。有不少黑客袭击网络时并不是怀有恶意，他们多数情况下只是为了表现和证实自己在计算机方面的天分与才华，但也有一些黑客的网络袭击行为是有意地对网络进行破坏。

黑客（Hacker）指那些利用技术手段进入其权限以外计算机系统的人。在虚拟的网络世界里，活跃着这批特殊的人，他们是真正的程序员，有过人的才能和乐此不疲的创造欲。技术的进步给了他们充分表现自我的天地，同时也使计算机网络世界多了一份灾难，一般人们把他们称之为黑客（Hacker）或骇客（Cracker），前者更多指的是具有反传统精神的程序员，后者更多指的是利用工具攻击别人的攻击者，具有明显贬义。但无论是黑客还是骇客，都是具备高超的计算



机知识的人。目前世界最著名的黑客组织有美国的大屠杀 2600（Genocide2600）、德国的混沌计算机俱乐部（Chaos Computer Club）、北美洲的地下兵团（The Legion of the Underground）等。在国外，更多的黑客是无政府主义者、自由主义者，而在国内，大部分黑客表现为民族主义者。近年来，国内陆续出现了一些自发组织的黑客团体，有“中国鹰派”、“绿色兵团”、“中华黑客联盟”等，其中的典型代表是“中国红客网络安全技术联盟（Honker Union of China）”，简称 H. U. C，网址为 www. cnhonker. com。

黑客的攻击手段多种多样，下面列举一些常见的形式。

1. 口令入侵

所谓口令入侵是指使用某些合法用户的账号和口令登录到目的主机，然后再实施攻击活动。使用这种方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。

通常黑客会利用一些系统使用习惯性的账号的特点，采用字典穷举法（或称暴力法）来破解用户的密码。由于破译过程由计算机程序来自动完成，因而几分钟到几个小时之间就可以把拥有几十万条记录的字典里所有单词都尝试一遍。其实黑客能够得到并破解主机上的密码文件，一般都是利用系统管理员的失误。在 UNIX 操作系统中，用户的基本信息都存放在 passwd 文件中，而所有的口令则经过 DES 加密方法加密后专门存放在一个叫 shadow 的文件中。黑客们获取口令文件后，就会使用专门的破解 DES 加密法的程序来破解口令。同时，由于为数不少的操作系统都存在许多安全漏洞、Bug 或一些其他设计缺陷，这些缺陷一旦被找出，黑客就可以长驱直入。例如，让 Windows 系统后门洞开的特洛伊木马程序（Trojan Horse）就是利用了 Windows 的基本设计缺陷。

采用中途截击的方法也是获取用户账户和密码的一条有效途径。因为很多协议没有采用加密或身份认证技术，如在 Telnet、FTP、HTTP、SMTP 等传输协议中，用户账户和密码信息都是以明文格式传输的，此时若攻击者利用数据包截取工具便可以很容易地收集到账户和密码。还有一种中途截击的攻击方法，它可以在用户同服务器端完成“三次握手”建立连接之后，在通信过程中扮演“第三者”的角色，假冒服务器身份欺骗用户，再假冒用户向服务器发出恶意请求，其造成的后果不堪设想。另外，黑客有时还会利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码，或者使用有缓冲区溢出错误的 SUID 程序来获得超级用户权限。

2. 放置特洛伊木马程序

在古希腊人同特洛伊人的战争期间，古希腊人佯装撤退并留下一只内部藏有士兵的巨大木马，特洛伊人大意中计，将木马拖入特洛伊城。夜晚木马中的希腊士兵出来与城外战士里应外

合，攻破了特洛伊城，特洛伊木马的名称也就由此而来。在计算机领域里，有一类特殊的程序，黑客通过它来远程控制别人的计算机，把这类程序称为特洛伊木马程序。从严格的定义来讲，凡是非法驻留在目标计算机里，在目标计算机系统启动的时候自动运行，并在目标计算机上执行一些事先约定的操作，比如窃取口令等，这类程序都可以称为特洛伊木马程序。

特洛伊木马程序一般分为服务器端（Server）和客户端（Client），服务器端是攻击者传到目标机器上的部分，用来在目标机上监听等待客户端连接过来。客户端是用来控制目标机器的部分，放在攻击者的机器上。

特洛伊木马程序常被伪装成工具程序或游戏，一旦用户打开了带有特洛伊木马程序的邮件附件或从网上直接下载，或执行了这些程序之后，当用户连接到因特网上时，这个程序就会把用户的 IP 地址及被预先设定的端口通知黑客。黑客在收到这些资料后，再利用这个潜伏其中的程序，就可以恣意修改用户的计算机设定，复制文件，窥视用户整个硬盘内的资料等，从而达到控制用户计算机的目的。现在有许多这样的程序，国外的此类软件有 Back Oriffice、Netbus 等，国内的此类软件有 Netspy、YAI、SubSeven、冰河、“广外女生”等。

3. DoS 攻击

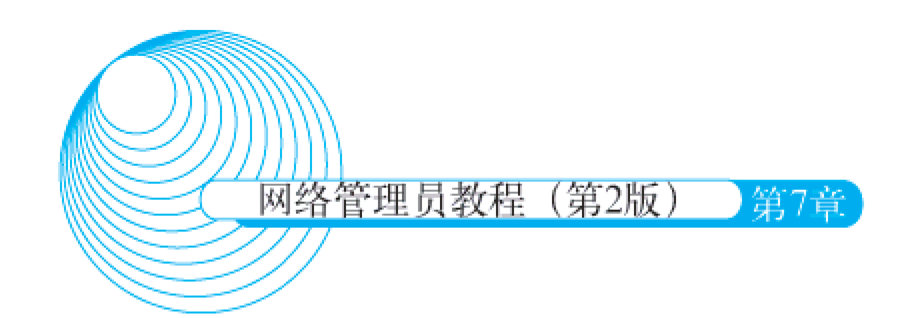
DoS 是 Denial of Service 的简称，即拒绝服务，造成 DoS 的攻击行为被称为 DoS 攻击，其目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过。连通性攻击是指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。

分布式拒绝服务（DDoS，Distributed Denial of Service）攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃账号将 DDoS 主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通信，代理程序已经被安装在因特网上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

4. 端口扫描

所谓端口扫描，就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等，从而侦知目标主机的扫描端口是否处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等。常用的扫描方式有：TCP connect( )扫描、TCP SYN 扫描、TCP FIN 扫描、IP 段扫描和 FTP 返回攻击等。

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器可以不留痕迹



的发现远程服务器的各种 TCP 端口的分配及提供的服务和它们的软件版本。扫描器并不是一个直接的攻击网络漏洞的程序，它仅能发现目标主机的某些内在的弱点。一个好的扫描器能对它得到的数据进行分析，帮助用户查找目标主机的漏洞。但它不会提供进入一个系统的详细步骤。扫描器应该有 3 项功能：发现一个主机或网络的能力；一旦发现一台主机，有发现什么服务正运行在这台主机上的能力；通过测试这些服务，发现漏洞的能力。

5. 网络监听

网络监听，在网络安全上一直是一个比较敏感的话题，作为一种发展比较成熟的技术，监听在协助网络管理员监测网络传输数据、排除网络故障等方面具有不可替代的作用，因而一直备受网络管理员的青睐。然而，在另一方面网络监听也给以太网的安全带来了极大的隐患，许多的网络入侵往往都伴随着以太网内的网络监听行为，从而造成口令失窃、敏感数据被截获等连锁性安全事件。

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具就可轻而易举地截取包括口令和账号在内的信息资料。

Sniffer 是一个著名的监听工具，它可以监听到网上传输的所有信息。Sniffer 可以是硬件也可以是软件，主要用来接收在网络上传输的信息。Sniffer 可以使用在任何一种平台之中，在使用 Sniffer 时，极不容易被发现，它可以截获口令，也可以截获到本来是秘密的或者专用信道内的信息，例如信用卡号、经济数据、E-mail 等，甚至可以用来攻击与自己相邻的网络。在 Sniffer 中，还有“热心人”编写了它的 Plugin，称为 TOD 杀手，可以将 TCP 的连接完全切断。总之，Sniffer 是个非常危险的软件，应该引起人们的重视。

6. 欺骗攻击

欺骗攻击是攻击者创造一个易于误解的上下文环境，以诱使受攻击者进入并且作出缺乏安全考虑的决策。欺骗攻击就像是一场虚拟游戏：攻击者在受攻击者的周围建立起一个错误但是令人信服的世界。如果该虚拟世界是真实的话，那么受攻击者所做的一切都是无可厚非的。但遗憾的是，在错误的世界中似乎是合理的活动可能会在现实的世界中导致灾难性的后果。常见的欺骗攻击有：

(1) Web 欺骗。Web 欺骗允许攻击者创造整个 WWW 世界的影像复制。影像 Web 的入口进入到攻击者的 Web 服务器，经过攻击者机器的过滤作用，允许攻击者监控受攻击者的任何活动，包括账户和口令。攻击者也能以受攻击者的名义将错误或者易于误解的数据发送到真正的 Web 服务器，以及以任何 Web 服务器的名义发送数据给受攻击者。简而言之，攻击者观察和控

制着受攻击者在 Web 上做的每一件事。

(2) ARP 欺骗。通常源主机在发送一个 IP 包之前，它要到该转换表中寻找和 IP 包对应的 MAC 地址。此时，若入侵者强制目的主机 Down 掉（比如发洪水包），同时把自己主机的 IP 地址改为合法目的主机的 IP 地址，然后他发一个 ping(icmp 0)给源主机，要求更新主机的 ARP 转换表，主机找到该 IP，然后在 ARP 表中加入新的 IP 与 MAC 对应关系。合法的目的主机失效了，入侵主机的 MAC 地址变成了合法的 MAC 地址。

(3) IP 欺骗。IP 欺骗由若干步骤组成。首先，目标主机已经选定。其次，信任模式已被发现，并找到了一个被目标主机信任的主机。黑客为了进行 IP 欺骗，进行以下工作：使得被信任的主机丧失工作能力，同时采样目标主机发出的 TCP 序列号，猜测出它的数据序列号。然后，伪装成被信任的主机，同时建立起与目标主机基于地址验证的应用连接。如果成功，黑客可以使用一种简单的命令放置一个系统后门，以进行非授权操作。

7. 电子邮件攻击

电子邮件攻击主要表现为向目标信箱发送电子邮件炸弹。所谓的邮件炸弹实质上就是发送地址不详且容量庞大的邮件垃圾。由于邮件信箱都是有限的，当庞大的邮件垃圾到达信箱的时候，就会把信箱挤爆。同时，由于它占用了大量的网络资源，常常导致网络塞车，它常发生在当某人或某公司的所作所为引起了某些黑客的不满时，黑客就会通过这种手段来发动进攻，以泄私愤。因为相对于其他攻击手段来说，这种攻击方法具有简单、见效快等优点。

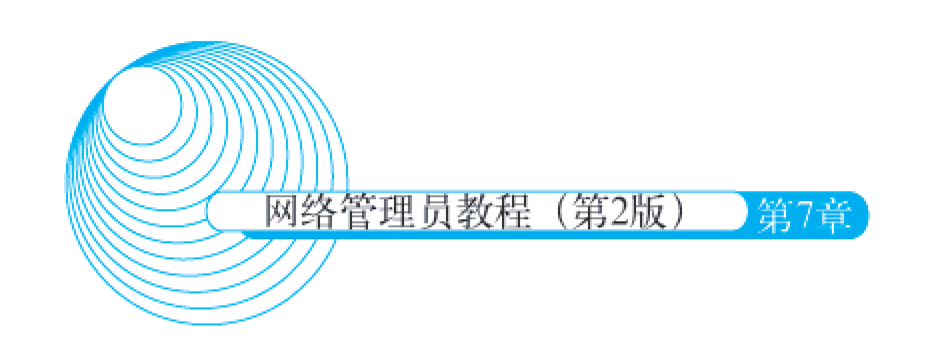
此外，电子邮件欺骗也是黑客常用的手段。他们常会佯称自己是系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令有可能为指定的字符串）或在貌似正常的附件中加载病毒或某些特洛伊木马程序。

8. 社会工程学攻击

社会工程学是关于建立理论通过自然的、社会的和制度上的途径并特别强调根据现实的双向计划和设计经验来一步接一步地解决各种社会问题。社会工程学攻击，是攻击者利用人际关系的互动性所发出的攻击。通常攻击者如果无法通过物理入侵直接取得所需要的资料时，就会通过电子邮件或者电话对所需要的资料进行骗取，再利用这些资料获取主机的权限以达到其本身的目的。

7.1.3 可信计算机系统评估标准

当前，计算机网络系统和计算机信息系统的建设者、管理者和使用者都面临着一个共同的问题，就是他们建设、管理或使用的信息系统是否是安全的？如何评估系统的安全性？这就需要有一整套用于规范计算机信息系统安全建设和使用的标准和管理办法。



1. 计算机系统安全评估准则综述

计算机系统安全评估准则是一种技术性法规。在信息安全这一特殊领域，如果没有这一标准，与此相关的立法、执法就会有失偏颇，最终会给国家的信息安全带来严重后果。由于信息安全产品和系统的安全评估事关国家的安全利益，因此许多国家都在充分借鉴国际标准的前提下，积极制订本国的计算机安全评估认证标准。

美国国防部早在20世纪80年代就针对国防部门的计算机安全保密开展了一系列有影响的工作，后来成立了所属的机构——国家计算机安全中心(NCSC)继续进行有关工作。1983年他们公布了可信计算机系统评估准则(TCSEC，Trusted Computer System Evaluation Criteria，俗称桔皮书)，桔皮书中使用了可信计算基础(TCB，Trusted Computing Base)这一概念，即计算机硬件与支持不可信应用及不可信用户的操作系统的组合体。在TCSEC的评估准则中，从B级开始就要求具有强制存取控制和形式化模型技术的应用。桔皮书论述的重点是通用的操作系统，为了使它的评判方法适用于网络，NCSC于1987年出版了一系列有关可信计算机数据库、可信计算机网络指南等(俗称彩虹系列)。该书从网络安全的角度出发，解释了准则中的观点，从用户登录、授权管理、访问控制、审计跟踪、隐通道分析、可信通道建立、安全检测、生命周期保障、文本写作、用户指南均提出了规范性要求，并根据所采用的安全策略、系统所具备的安全功能将系统分为4类7个安全级别，将计算机系统的可信程度划分为D1、C1、C2、B1、B2、B3和A1 7个层次。

TCSEC带动了国际计算机安全的评估研究，90年代西欧4国(英、法、荷、德)联合提出了信息技术安全评估标准(ITSEC，Information Technology System Evaluation Criteria，又称欧洲白皮书)，ITSEC除了借鉴TCSEC的成功经验外，首次提出了信息安全的保密性、完整性、可用性的概念，把可信计算机的概念提高到可信信息技术的高度上来认识。他们的工作成为欧共体信息安全计划的基础，并对国际信息安全的研究、实施带来深刻的影响。

ITSEC标准将安全概念分为功能与评估两部分。功能准则从F1～F10共分10级。F1～F5级对应于TCSEC的D到A。F6～F10级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性以及机密性和完整性的网络安全。评估准则分为6级，分别是测试、配置控制和可控的分配、能访问详细设计和源码、详细的脆弱性分析、设计与源码明显对应以及设计与源码在形式上一致。

1993年，加拿大发布了“加拿大可信计算机产品评估准则”(CTCPEC，Canada Trusted Computer Product Evaluation Criteria)，CTCPEC综合了TCSEC和ITSEC两个准则的优点，专门针对政府需求而设计。与ITSEC类似，该标准将安全分为功能性需求和保证性需要两部分。功能性需求共划分为4大类：机密性、完整性、可用性和可控性。每种安全需求又可以分成很多小类，来表示安全性上的差别，级别为0～5级。

1993 年同期，美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上，发布了“信息技术安全评估联邦准则”（FC，Federal Criteria）。FC 是对 TCSEC 的升级，并引入了“保护轮廓”（PP，Protect Profile）的概念。每个轮廓都包括功能、开发保证和评价 3 部分。FC 充分吸取了 ITSEC 和 CTCPEC 的优点，在美国的政府、民间和商业领域得到了广泛应用。

近年来，随着世界市场上对信息安全产品的需求迅速增长以及对系统安全的挑战不断加剧，6 国 7 方（美国国家安全局和国家技术标准研究所、加、英、法、德、荷）联合起来，在美国的 TCSEC、欧洲的 ITSEC、加拿大的 CTCPEC、美国的 FC 等信息安全准则的基础上，提出了“信息技术安全评价通用准则（CC，The Common Criteria for Information Technology Security Evaluation）”，它综合了过去信息安全的准则和标准，形成了一个更全面的框架。CC 主要面向信息系统的用户、开发者和评估者，通过建立这样一个标准，使用户可以用它来确定对各种信息产品的信息安全要求，使开发者可以用它来描述其产品的安全特性，使评估者可以对产品安全性的可信度进行评估。不过，CC 并不涉及管理细节和信息安全的具体实现、算法、评估方法等，也不作为安全协议、安全鉴定等，CC 的目的是形成一个关于信息安全的单一国际标准，从而使信息安全产品的开发者和信息安全产品能在全世界范围内发展。总之，CC 是安全准则的集合，也是构建安全要求的工具，对于信息系统的用户、开发者和评估者都有重要的意义。1996 年 6 月，CC 第 1 版发布；1998 年 5 月，CC 第 2 版发布；1999 年 10 月 CC v2.1 版发布，并且成为 ISO 标准。CC 的主要思想和框架都取自 ITSEC 和 FC，并充分突出了“保护轮廓”概念。CC 将评估过程划分为功能和保证两部分，评估等级分为 eal1、eal2、eal3、eal4、eal5、eal6 和 eal7 共 7 个等级。每一级均包括评估配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性等。

1999 年 5 月，国际标准化组织和国际电联（ISO/IEC）通过了将 CC 作为国际标准 ISO/IEC 15408 信息技术安全评估准则的最后文本。从 TCSEC、ITSEC 到 ISO/IEC 15408 信息技术安全评估准则中可以看出，评估准则不仅评估产品本身，而且还评估开发过程和使用操作，强调安全的全过程性。ISO/IEC 15408 的出台，表明了安全技术的发展趋势。

2. 可信计算机安全评估准则（TCSEC）

TCSEC 将计算机系统的安全划分为 4 个等级、7 个级别。

（1）D 类安全等级：D 类安全等级只包括 D1 一个级别。D1 是安全等级最低的一个级别。D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。

（2）C 类安全等级：该类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。C1 系统的可信计算基础体制通过将用户和数据分开来达到安全的目的。在 C1 系统中，所有的用户以同样的灵敏度来处理数据，即用户认为

C1 系统中的所有文档都具有相同的机密性。C2 系统比 C1 系统加强了可调的审慎控制。在连接到网络上时，C2 系统的用户分别对各自的行为负责。C2 系统通过登录过程、安全事件和资源隔离来增强这种控制。C2 系统具有 C1 系统中所有的安全性特征。

(3) B 类安全等级：B 类安全等级可分为 B1、B2 和 B3 3 类。B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B1 系统满足下列要求：

- 系统对网络控制下的每个对象都进行灵敏度标记；
- 系统使用灵敏度标记作为所有强迫访问控制的基础；
- 系统在把导入的、非标记的对象放入系统前标记它们；
- 灵敏度标记必须准确地表示其所联系的对象的安全级别；
- 当系统管理员创建系统或者增加新的通信通道或 I/O 设备时，管理员必须指定每个通信通道和 I/O 设备是单级还是多级，并且管理员只能手工改变指定；
- 单级设备并不保持传输信息的灵敏度级别；
- 所有直接面向用户位置的输出（无论是虚拟的还是物理的）都必须产生标记来指示关于输出对象的灵敏度；
- 系统必须使用用户的口令或证明来决定用户的安全访问级别；
- 系统必须通过审计来记录未授权访问的企图。

B2 系统必须满足 B1 系统的所有要求。另外，B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信计算基础体制。B2 系统必须满足下列要求：

- 系统必须立即通知系统中的每一个用户所有与之相关网络连接的改变；
- 只有用户才能在可信任通信路径中进行初始化通信；
- 可信任运算基础体制能够支持独立的操作者和管理员。

B3 系统必须符合 B2 系统的所有安全需求。B3 系统具有很强的监视委托管理访问能力和抗干扰能力。B3 系统必须设有安全管理员。B3 系统应满足以下要求：

- 除了控制对个别对象的访问外，B3 必须产生一个可读的安全列表；
- 每个被命名的对象提供对该对象没有访问权的用户列表说明；
- 系统在进行任何操作前，都要求用户进行身份验证；
- 系统验证每个用户，同时还会发送一个取消访问的审计跟踪消息；
- 设计者必须正确区分可信任的通信路径和其他路径；
- 可信任的通信基础体制为每一个被命名的对象建立安全审计跟踪；
- 可信任的运算基础体制支持独立的安全管理。

(4) A 类安全等级：A 系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是，系统的设

计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：

- 系统管理员必须从开发者那里接收到一个安全策略的正式模型；
- 所有的安装操作都必须由系统管理员进行；
- 系统管理员进行的每一步安装操作都必须有正式文档。

3. 我国计算机信息系统安全保护等级划分准则

长期以来，我国一直十分重视信息安全保密工作，并从敏感性、特殊性和战略性的高度，自始至终将其置于国家的绝对领导之下，由国家密码管理部门、国家安全机关、公安机关和国家保密主管部门等分工协作，各司其职，形成了维护国家信息安全的管理体系。

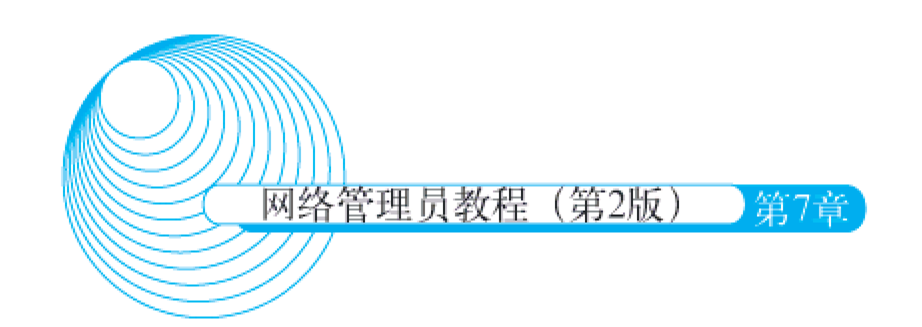
1999 年 2 月 9 日，为更好地与国际接轨，经国家质量技术监督局批准，正式成立了“中国国家信息安全测评认证中心（CNISTECC，China National Information Security Testing Evaluation Certification Center）”。1994 年，国务院发布了《中华人民共和国计算机信息系统安全保护条例》，该《条例》是计算机信息系统安全保护的法律基础。其中第九条规定“计算机信息系统实行安全等级保护。安全等级的划分和安全等级的保护的具体办法，由公安部会同有关部门制订”。公安部在该《条例》发布实施后组织制订了《计算机信息系统安全保护等级划分准则》（GB 17859—1999），并于 1999 年 9 月 13 日由国家质量技术监督局审查通过并正式批准发布，已于 2001 年 1 月 1 日起执行。该《准则》的发布为我国计算机信息系统安全法规和配套标准制订的执法部门的监督检查提供了依据，为安全产品的研制提供了技术支持，为安全系统的建设和管理提供了技术指导，是我国计算机信息系统安全保护等级工作的基础。本标准规定了计算机系统安全保护能力的 5 个等级。

（1）第 1 级：用户自主保护级（对应 TCSEC 的 C1 级）。本级的计算机信息系统可信计算基础通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。

（2）第 2 级：系统审计保护级（对应 TCSEC 的 C2 级）。与用户自主保护级相比，本级的计算机信息系统可信计算基础实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

（3）第 3 级：安全标记保护级（对应 TCSEC 的 B1 级）。本级的计算机信息系统可信计算基础具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。

（4）第 4 级：结构化保护级（对应 TCSEC 的 B2 级）。本级的计算机信息系统可信计算基础



建立于一个明确定义的形式化安全策略模型之上，它要求将第3级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基础必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基础的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。它加强了鉴别机制，支持系统管理员和操作员的职能，提供可信设施管理，增强了配置管理控制。系统具有相当的抗渗透能力。

（5）第5级：访问验证保护级（对应TCSEC的B3级）。本级的计算机信息系统可信计算基础满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。

- 访问监控器本身是抗篡改的，必须足够小，能够分析和测试。
- 为了满足访问监控器需求，计算机信息系统可信计算基础在其构造时，排除那些对实施安全策略来说并非必要的代码，在设计和实现时，从系统工程角度将其复杂性降低到最小程度。
- 支持安全管理员职能，扩充审计机制，当发生与安全相关的事件时发出信号，提供系统恢复机制。
- 系统具有很高的抗渗透能力。

7.2 防火墙

7.2.1 防火墙简介

1. 防火墙的定义

在人们建筑和使用木制结构房屋的时候，为了在“城门失火”时不致“殃及池鱼”，就将坚固的石块堆砌在房屋周围作为屏障以防止火灾的发生和蔓延，这种防护构筑物被称之为“防火墙”，这是防火墙的本义。在当今的信息世界里，人们借助了这个概念，使用防火墙来保护敏感的数据不被窃取和篡改，不过这些防火墙是由先进的计算机硬件或软件系统构成的。简单地说，防火墙是位于两个信任程度不同的网络之间的软件或硬件设备的组合，如图7-1所示。它对两个或多个网络之间的通信进行控制，通过强制实施统一的安全策略，防止对重要信息资源的非法存取和访问，以达到保护系统安全的目的。

防火墙通常是运行在一台单独计算机之上的一个特别的服务软件，用来保护由许多台计算机组成的内部网。它使企业的网络规划清晰明了，它可以识别并屏蔽非法请求，有效防止跨越权限的数据访问。它既可以是非常简单的过滤器，也可能是精心配置的网关，但它们的原理是一样的，都是监测并过滤所有内部网和外部网之间的信息交换。防火墙保护着内部网的敏感数据不被窃取和破坏，并记录内外通信的有关状态信息日志，如通信发生的时间和进行的操作等。

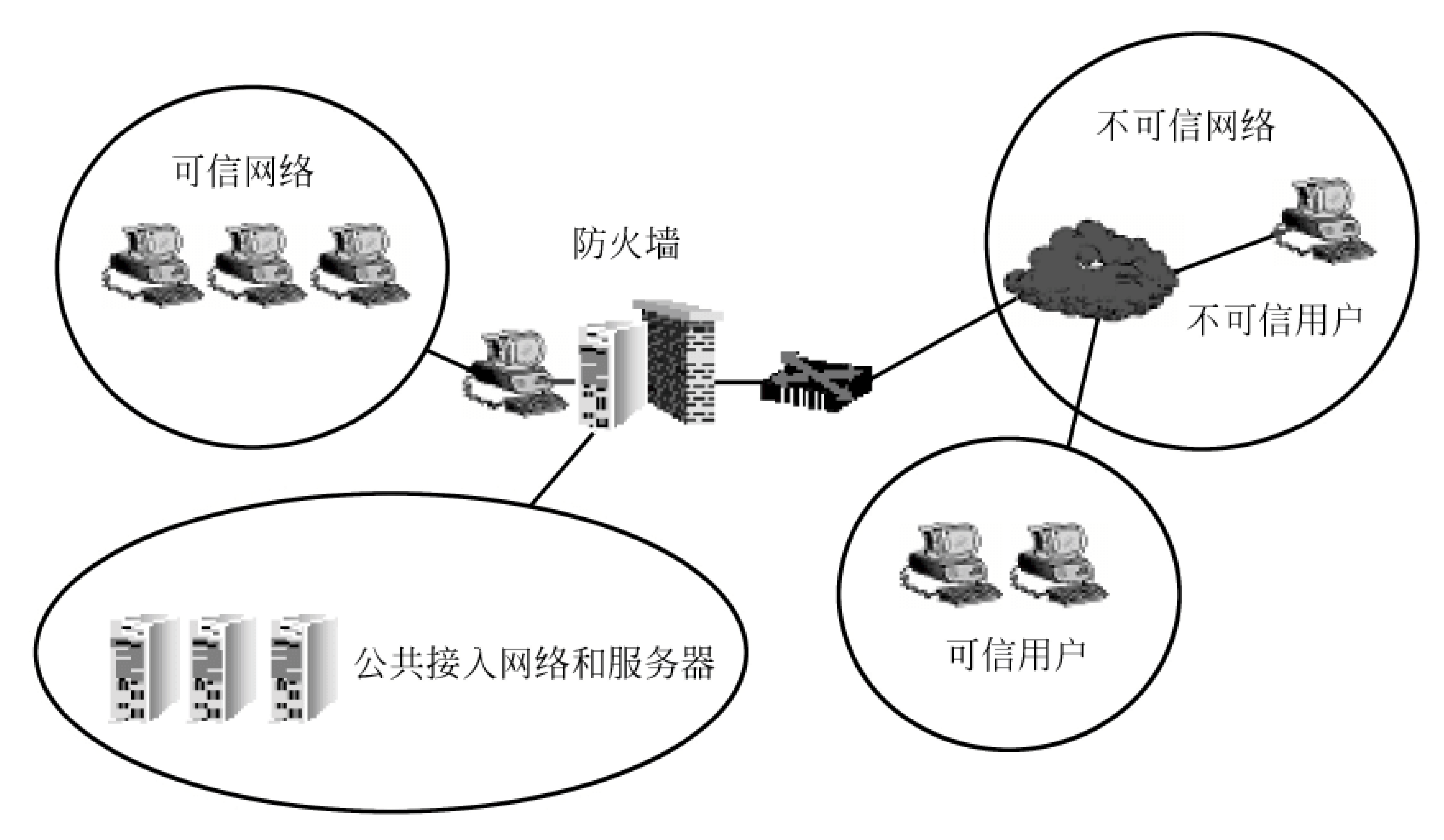


图 7-1　防火墙功能示意

新一代的防火墙甚至可以阻止内部人员将敏感数据向外传输。即使在公司内部，同样也存在这种数据非法存取的可能性。设置了防火墙以后，就可以对网络数据的流动实现有效地管理：允许公司内部员工使用电子邮件、进行 Web 浏览以及文件传输等服务，但不允许外界随意访问公司内部的计算机，同样还可以限制公司中不同部门之间互相访问，将局域网络放置于防火墙之后可以有效阻止来自外界的攻击。

防火墙是加强网络安全的一种非常流行的方法。在因特网的 Web 网站中，超过三分之一的网站都是由防火墙加以保护的，这是防范黑客攻击最安全的一种方式。从逻辑上讲，防火墙是分离器、限制器和分析器，它有效地监控了信任网络和非信任网络之间的任何活动，保证了信任网络的安全。从实现方式上防火墙可以分为硬件防火墙和软件防火墙两类，硬件防火墙是通过硬件和软件的组合来达到隔离内、外部网络的目的；软件防火墙是通过纯软件的方式来实现隔离内、外部网络的目的。

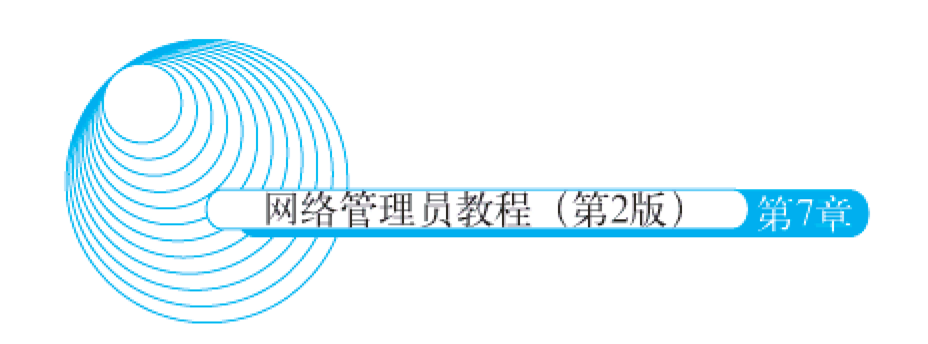
防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域（即非信任网络）与安全区域（信任网络）的连接，同时不会影响人们对风险区域的访问。防火墙的作用是监控进出网络的信息，仅让安全的、符合规则的信息进入内部网，为用户提供一个安全的网络环境。通常的防火墙具有以下一些功能：

（1）对进出的数据包进行过滤，滤掉不安全的服务和非法用户。

（2）监视因特网安全，对网络攻击行为进行检测和报警。

（3）记录通过防火墙的信息内容和活动。

（4）控制对特殊站点的访问，封堵某些禁止的访问行为。



2. 防火墙的相关概念

除了防火墙的概念外，有必要了解一些防火墙的相关概念。

(1) 非信任网络(公共网络)：处于防火墙之外的公共开放网络，一般指因特网。

(2) 信任网络(内部网络)：位于防火墙之内的可信网络，是防火墙要保护的目标。

(3) DMZ(非军事化区)：也称周边网络，可以位于防火墙之外也可以位于防火墙之内。安全敏感度和保护强度较低。非军事化区一般用来放置提供公共网络服务的设备。这些设备由于必须被公共网络访问，所以无法提供与内部网主机相等的安全性。

(4) 可信主机：位于内部网的主机，且具有可信任的安全特性。

(5) 非可信主机：不具有可信特性的主机。

(6) 公网 IP 地址：有因特网信息中心统一管理分配的 IP 地址。可在因特网上使用。

(7) 保留 IP 地址：专门保留用于内部网的 IP 地址，可以由网络管理员任意指派，在因特网上不可识别和不可路由，如：192.168.0.0 和 10.0.0.0 等地址网段。

(8) 包过滤：防火墙对每个数据包进行允许或拒绝的决定，具体地说，就是根据数据包的头部按照规则进行判断，决定继续转发还是丢弃。

(9) 地址转换：防火墙将内部网主机不可路由的保留地址转换成公共网络可识别的公共地址，可以达到节省 IP 和隐藏内部网拓扑结构信息等目的。

3. 防火墙的优、缺点

防火墙是加强网络安全的一种有效手段，它有以下优点：

(1) 防火墙能强化安全策略。因特网上每天都有几百万人在浏览信息，不可避免的会有心怀恶意的黑客试图攻击别人，防火墙充当了防止攻击现象发生的“网络巡警”，它执行系统规定的策略，仅允许符合规则的信息通过。

(2) 防火墙能有效的记录因特网上的活动。因为所有进出的信息都需要经过防火墙，所以防火墙可以记录信任网络和非信任网络之间发生的各种事件。

(3) 防火墙是一个安全策略的边防站。所有进出内部网的信息都必须通过防火墙，防火墙便成为一个安全检查站，能够把可疑的连接或者访问拒之门外。

有人认为只要安装了防火墙，就会解决网络内所有的安全问题。实际上，防火墙并不是万能的，安装了防火墙的系统依然存在着安全隐患。以下是防火墙的一些缺点：

(1) 防火墙不能防范不经由防火墙的攻击。例如，如果允许从受保护网内部不受限制的向外拨号，一些用户可以形成与因特网直接的连接，从而绕过防火墙，造成一个潜在的后门攻击渠道。

(2) 防火墙不能防止感染了病毒的软件或文件的传输。解决这个问题还需防病毒系统。

（3）防火墙不能防止数据驱动式攻击。当有些表面看来无害的数据被邮寄或复制到因特网主机上并被执行而发起攻击时，就会发生数据驱动攻击。因此，防火墙只是一种整体安全防范政策的一部分。这种安全政策必须包括公开的、以便用户知道自身责任的安全准则、职员培训计划以及与网络访问、当地和远程用户认证、拨出拨入呼叫、磁盘和数据加密以及病毒防护的有关政策。

7.2.2 防火墙基本分类及实现原理

根据防火墙实现原理的不同，通常将防火墙分为包过滤防火墙、应用层网关防火墙和状态检测防火墙 4 类。

1. 包过滤防火墙

包过滤防火墙是在网络的入口对通过的数据包进行选择，只有满足条件的数据包才能通过，否则被抛弃。包过滤防火墙如图 7-2 所示。

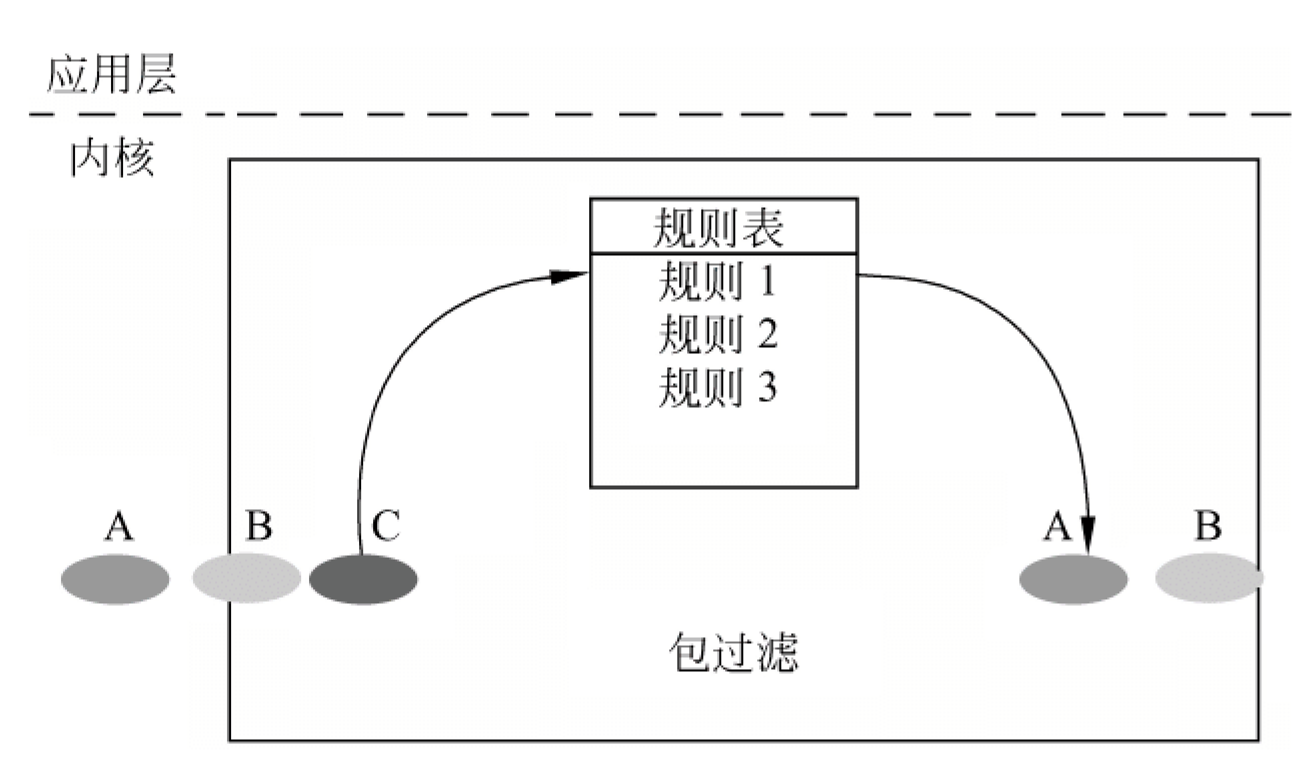


图 7-2 包过滤防火墙示意

本质上说，包过滤防火墙是多址的，表明它有两个或两个以上网络适配器或接口。例如，作为防火墙的设备可能有 3 块网卡，一块连到内部网，一块连到公共的因特网，另外一块连接到 DMZ。防火墙的任务，就是作为“网络警察”，指引包和截住那些有危害的包。包过滤防火墙检查每一个传入包，查看包中可用的基本信息，包括源地址、目的地址、TCP/UDP 端口号、传输协议（TCP、UDP、ICMP 等）。然后，将这些信息与设立的规则相比较。如果已经设立了拒绝 TELNET 连接，而包的目的端口是 23，那么该包就会被丢弃。如果允许传入 Web 连接，而目的端口为 80，则包就会被放行。

包过滤防火墙中每个 IP 包的字段都会被检查，例如源地址、目的地址、协议、端口等。防火墙将基于这些信息应用过滤规则，与规则不匹配的包就被丢弃，如果有理由让该包通过，就要建立规则来处理它。包过滤防火墙是通过规则的组合来完成复杂策略的。例如，一个规则可以包

括："允许 Web 连接"、"但只针对指定的服务器"、"只针对指定的目的端口和目的地址"这样 3 个子规则。

包过滤技术的优点是简单实用，实现成本较低，在应用环境比较简单的情况下，能够以较小的代价在一定程度上保证系统的安全。但包过滤技术的缺陷也是明显的。包过滤技术是一种完全基于网络层的安全技术，只能根据数据包的来源、目标和端口等网络信息进行判断，无法识别基于应用层的恶意侵入，如恶意的 Java 小程序以及电子邮件中附带的病毒。有经验的黑客很容易伪造 IP 地址，骗过包过滤型防火墙。

2. 应用层网关防火墙

应用层网关防火墙又称代理(Proxy)，实际上并不允许在它连接的网络之间直接通信。相反，它是接受来自内部网特定用户应用程序的通信，然后建立与公共网络服务器单独的连接，如图 7-3 所示。

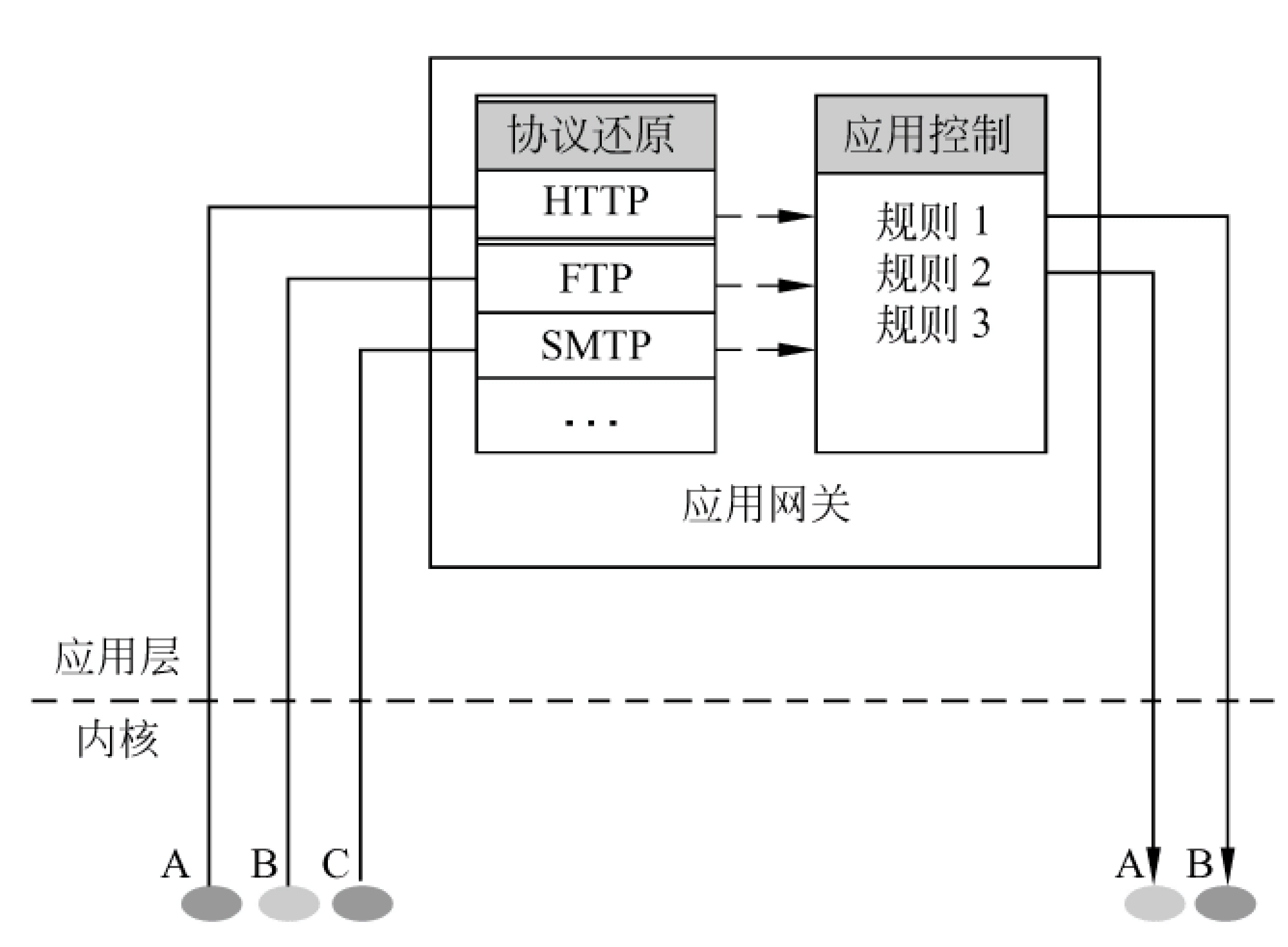


图 7-3　应用网关防火墙示意

网络内部的用户不直接与外部的服务器通信，所以服务器不能直接访问内部网的任何一部分。另外，如果不为特定的应用程序安装代理程序代码，这种服务是不会被支持的，不能建立任何连接。这种建立方式拒绝任何没有明确配置的连接，从而提供了额外的安全性和控制性。

例如，一个用户的 Web 浏览器可能在 80 端口，但也经常可能是在 1080 端口，连接到了内部网的 HTTP 代理防火墙。防火墙接受连接请求后，把它转到所请求的 Web 服务器。这种连接和转移对该用户来说是透明的，因为它完全是由代理防火墙自动处理的。代理防火墙通常支持的一些常见的应用程序有 HTTP、HTTPS/SSL、SMTP、POP3、IMAP、NNTP、TELNET、FTP、

IRC 等，目前国内很多厂家在硬件防火墙里集成这些模块，如北大方正公司的方正方御防火墙就能代理以上应用程序。

应用程序代理防火墙可以配置成允许来自内部网的任何连接，它也可以配置成要求用户认证后才建立连接，为安全性提供了额外的保证。如果网络受到危害，这个特征使得从内部发动攻击的可能性减少。

代理型防火墙的优点是安全性较高，可以针对应用层进行侦测和扫描，对付基于应用层的侵入和病毒都十分有效。其缺点是对系统的整体性能有较大的影响，而且代理服务器必须针对客户机可能产生的所有应用类型逐一进行设置，大大增加了系统管理的复杂性。

3. 状态检测防火墙

状态检测防火墙又称动态包过滤防火墙，是在传统包过滤上的功能扩展，现在已经成为防火墙的主流技术。状态检测防火墙如图 7-4 所示。

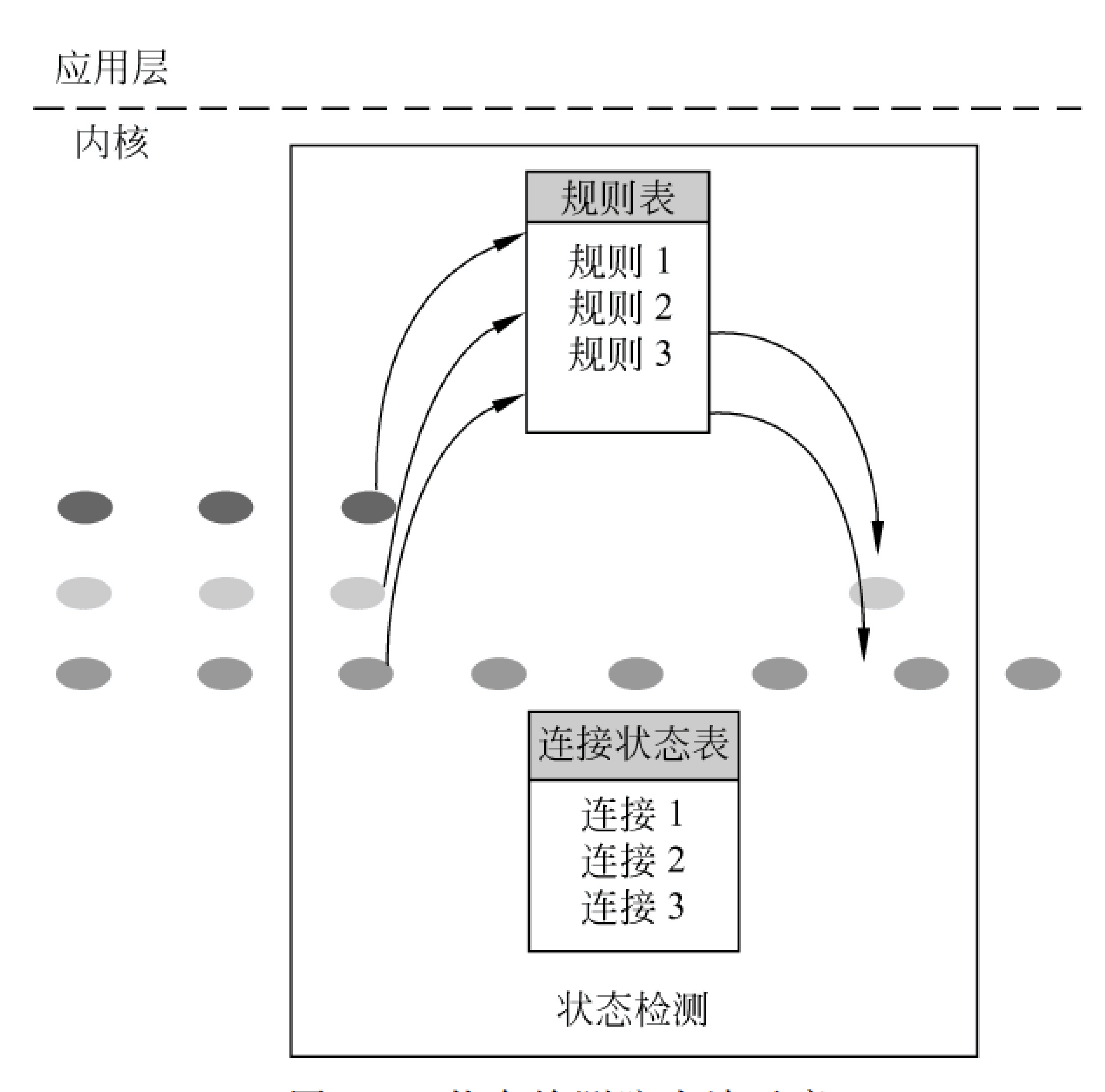


图 7-4 状态检测防火墙示意

有人将状态检测防火墙称为第三代防火墙，可见其应用的广泛性。相对于状态检测包过滤，将传统的包过滤称为静态包过滤，静态包过滤将每个数据包进行单独分析，固定地根据其包头信息进行匹配，这种方法在遇到利用动态端口应用协议时会发生困难。

FTP 在整个过程中使用了两种 TCP 连接，控制连接用于客户端与服务器端之间交互协商与命令传输，数据连接用于客户端与服务器端之间传输文件数据。客户端向服务器端固定的 21

端口发起连接请求建立控制连接，防火墙的静态包过滤根据这个固定的端口信息，很好地对控制连接实施过滤功能。而数据连接则使用动态端口，它是由控制连接来协商并发起，先由客户端或者服务器端在控制连接上发送 PORT 命令，将需要建立的动态端口作为参数传递，通过这种方式使客户端和服务器端完成了动态端口的协定。动态端口意味着每次的端口都有可能不一样，而防火墙无法知道哪些端口需要打开，如果采用原始的静态包过滤，又希望用到此服务的话，就需要将所有可能的端口打开，这会给安全带来不必要的隐患。而状态检测通过检查跟踪应用程序信息（如 FTP 的 PORT 命令），判断是否需要临时打开某个端口，当传输结束时，端口又马上恢复关闭状态。

状态检测防火墙，试图跟踪通过防火墙的网络连接和数据包，这样防火墙就可以使用一组附加的标准，以确定是允许还是拒绝通信。它是在使用了基本包过滤防火墙的通信上应用一些技术来做到这点的。

当包过滤防火墙见到一个网络包，包是孤立存在的，没有防火墙所关心的历史或未来。允许和拒绝包的决定完全取决于包自身所包含的信息，如源地址、目的地址、端口号等。包中没有包含任何描述它在信息流中的位置的信息，则该包被认为是无状态的，它仅是存在而已。一个有状态包检查的防火墙跟踪的不仅是包中包含的信息。为了跟踪包的状态，防火墙还记录有用的信息以帮助识别包，例如已经建立的或者相关的网络连接、数据的传出请求等。例如，如果传入的包包含视频数据流，而防火墙可能已经记录了有关信息，是关于位于特定 IP 地址的应用程序最近向发出包的源地址请求视频信号的信息。如果传入的包是要传给发出请求的相同系统，防火墙进行匹配，包就被允许通过。一个状态检测防火墙可截断所有传入的通信，而允许所有传出的通信。因为防火墙跟踪内部出去的请求，所有按要求传入的数据被允许通过，直到连接被关闭为止。只有未被请求的传入通信被截断。

跟踪连接状态的方式取决于通过防火墙包的类型：

（1）TCP 包。当建立起一个 TCP 连接时，通过的第一个包被标有包的 SYN 标志。通常情况下，防火墙丢弃所有外部的连接企图，除非已经建立起某条特定规则来处理它们。对内部的连接试图连到外部主机，防火墙注明连接包。在这种方式下，如果传入的包是响应一个已建立的连接时，才会被允许通过。

（2）UDP 包。UDP 包比 TCP 包简单，因为它们不包含任何连接或序列信息。它们只包含源地址、目的地址、校验和携带的数据，使得防火墙确定包的合法性很困难。可是，如果防火墙跟踪包的状态，就可以解决这个问题。对传入的包，若它所使用的地址和 UDP 包携带的协议与传出的连接请求匹配，该包就被允许通过。和 TCP 包一样，所有传入的 UDP 包都不会被允许通过，除非它是响应传出的请求或已经建立了指定的规则来处理它。对其他种类的包，情况和 UDP 包类似。防火墙仔细地跟踪传出的请求，记录下所使用的地址、协议和包的类型，然后对照保存过的信息核对传入的包，以确保这些包是被请求的。

状态检测防火墙是新一代的产品，这一技术实际已经超越了最初的防火墙定义。状态检测防火墙能够对多层的数据进行主动的、实时的监测，在对这些数据加以分析的基础上，检测型防火墙能够有效地判断出各层中的非法侵入。同时，这种检测型防火墙产品一般还带有分布式探测器，这些探测器安置在各种应用服务器和其他网络的节点之中，不仅能够检测来自网络外部的攻击，同时对来自内部的恶意破坏也有极强的防范作用。据权威机构统计，在针对网络系统的攻击中，有相当比例的攻击来自网络内部。因此，状态检测防火墙不仅超越了传统防火墙的定义，而且在安全性上也超越了前两代产品。

4. 复合型防火墙

复合型防火墙是指综合了状态检测与透明代理的新一代的防火墙，把内容过滤、邮件过滤等整合到防火墙里，其中还包括 VPN、IDS 功能，多单元融为一体，是一种新突破。常规的防火墙并不能防止隐蔽在网络流量里的攻击，在网络界面对应用层扫描，把内容过滤、邮件过滤与防火墙结合起来，这体现了网络与信息安全的新思路。它在网络边界实施第七层的内容扫描，实现了实时在网络边缘部署邮件防护、内容过滤等应用层服务措施。

如果从防火墙的软、硬件形式来分的话，防火墙可以分为软件防火墙、硬件防火墙以及芯片级防火墙。

(1) 软件防火墙

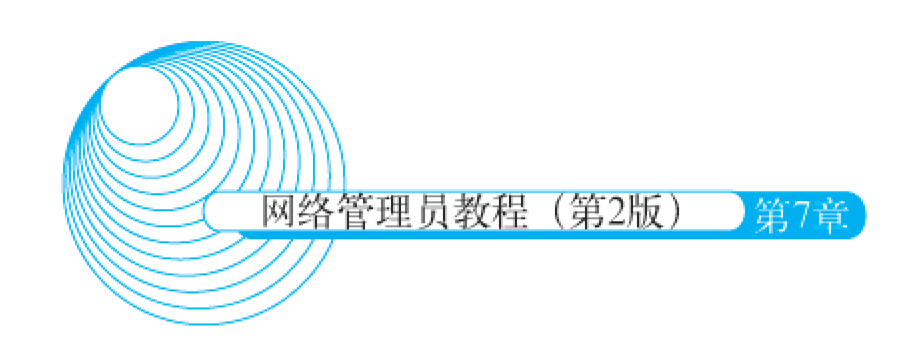
软件防火墙运行于特定的计算机上，它需要客户预先安装好操作系统，一般来说这台计算机就是整个网络的网关，俗称“个人防火墙”。软件防火墙就像其他的软件产品一样需要先在计算机上安装并做好配置才可以使用。使用这类防火墙，需要网管对所工作的操作系统平台比较熟悉。

(2) 硬件防火墙

硬件防火墙主要基于 x86 架构来进行设计的，x86 防火墙在灵活性和扩展性方面具有很大的优势。它采用通用的 CPU 和主板进行设计，产品功能主要由软件实现，很容易集成反病毒、内容过滤、计费、流量控制、对服务器远程监控等功能。不过，x86 架构的 CPU 为了支持复杂的运算并容易开发新的功能，采用了通用体系结构的指令集，所以其处理速度相对较慢，单个芯片的可扩展性较差，因而很难满足千兆网络对于高线速的需求。

(3) 芯片级防火墙

芯片级防火墙基于专门的硬件平台，没有操作系统，采用专有的 ASIC、NP 芯片，比其他种类的防火墙速度更快，处理能力更强，性能更高。如国内方正信息安全公司研发的 NP＋ASIC 防火墙突破了性能瓶颈。这类防火墙由于是专用 OS(操作系统)，因此防火墙本身的漏洞较少，不过价格相对较高。



7.2.3 防火墙系统安装与配置基础

目前，国内有很多厂家研制出自己的防火墙，如方正的方御防火墙、联想的网御防火墙等，国外的如 Cisco Pix、NetScreen 等硬件防火墙。下面仅以方正方御防火墙为例对防火墙的安装和配置加以说明。

1. 软硬件安装

方御防火墙的软件部分主要由管理监控程序（FireControl）、串口配置程序（FCInit）和日志报警程序（LogService）组成。FireControl 是方御的管理程序，其作用是管理、监控、配置方御和设置入侵攻击报警策略，进行设备管理和日常监控；FCInit 的主要功能是初始化 FG 防火墙，通过配置串口来完成一些初始化的工作；LogService 的功能是获取日志、提供日志报警信息，在程序的安装过程中，能够自动装载数据和文件，并在系统程序组中，生成方御防火墙的程序组。

方御的硬件名称为 FireGate，简称 FG。在硬件安装时，用电源线将 FireGate 接上电源，用网线将各网络接口连接到 FireGate 相应的网口上。硬件安装结构如图 7-5 所示。

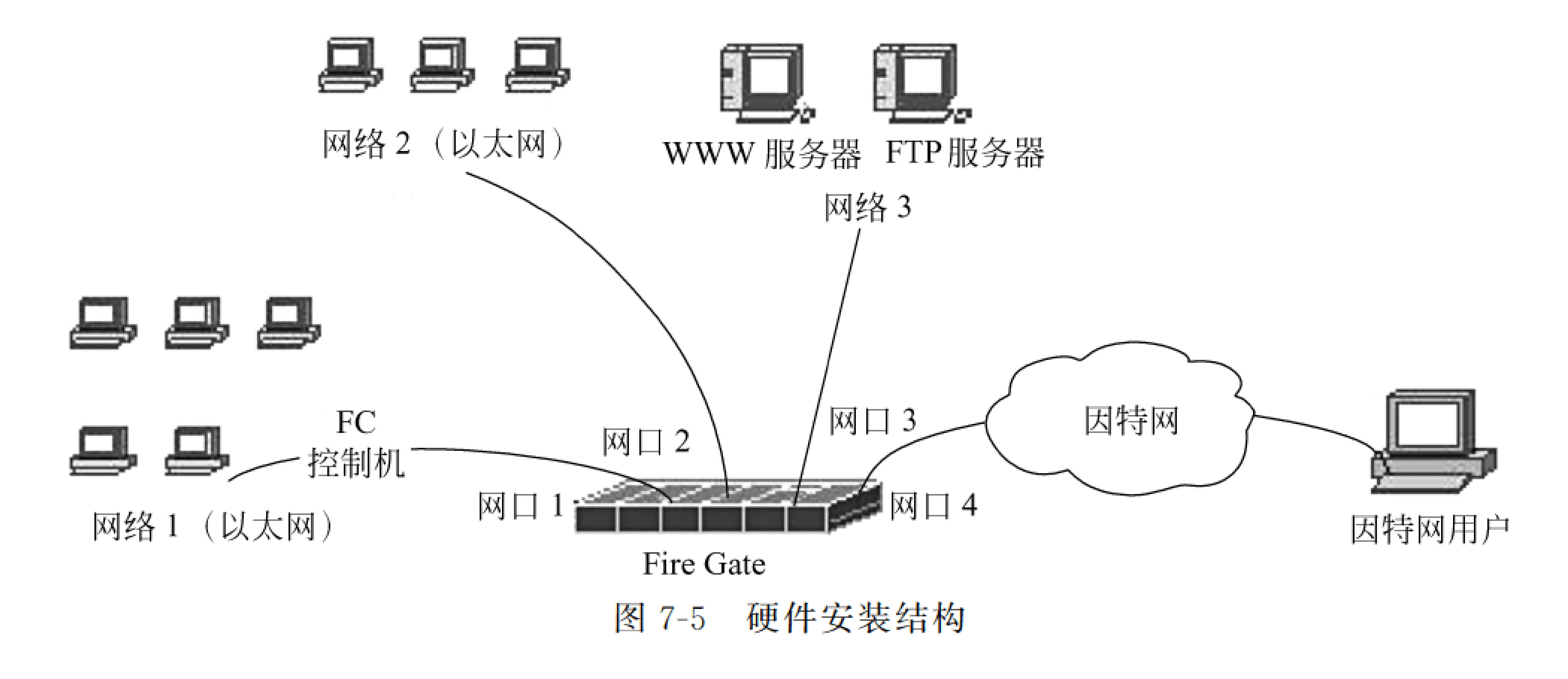
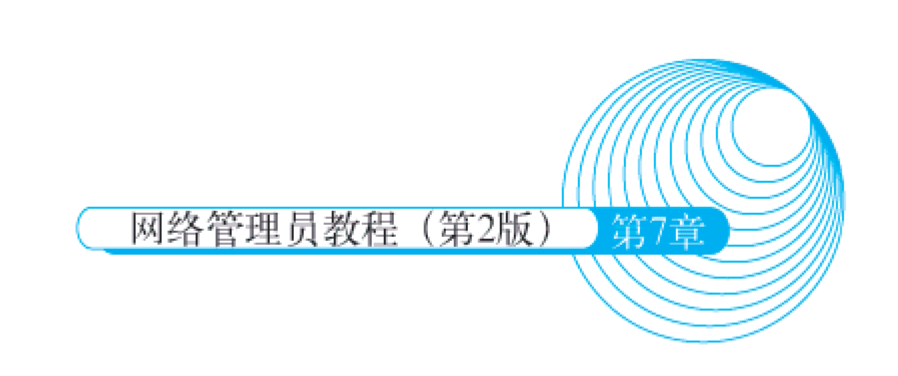


图 7-5 硬件安装结构

2. 基本配置

在 FireControl 安装程序完毕后，即可在桌面上找到它的快捷方式，FireControl 安装在控制机上，控制机可以是与 FireGate 网口相连的任意一台机器。

管理员第一次启动 FireControl 管理程序时，应使用在 FCInit 中新建实施域时创建的默认账号 admin 进行登录。登录成功以后，为安全起见，建议即刻修改 admin 账号的密码，以策略管理员身份登录 FireControl。策略管理员可自定义防火墙的各种参数，配置个性化的防火墙。防



火墙的基本配置包括以下几个方面：

1）别名

别名的设计是为了方便策略管理员的使用，策略管理员可以用好记的别名代替多个功能端口以及子网，使配置不再繁琐。例如使用别名 www 代替端口 80 或 8080，别名 office 代替 IP 地址为 105.118.0.0，子网掩码为 255.255.255.0 的网段地址，或者把几个离散的端口值或网段地址统一用一个别名进行管理。

别名是 FG 防火墙中重要的特性，大部分防火墙的功能模块配置都是通过别名来实现的，所以策略管理员需要事先定义好相关的网络地址和端口的别名。

2）设备配置

设备配置是防火墙自身的网络设置，包括对接口设备配置和显示防火墙基本信息。FG 初始化完成后，以策略管理员登录 FG，首先需要进行设备配置。用户可以根据自己实际的网络需求在设备配置模块中通过对网络接口设备的设置实现多种工作模式。防火墙可以有 3 种工作模式：桥模式、路由模式和混杂模式。另外，FG 还对 VLAN 提供充分支持。

（1）桥模式：如果用户不想改变原有的网络拓扑结构和设置，可以将防火墙设置成桥模式。在桥模式下，网络间的访问是透明的，所有网口设备将构成一个网桥。

（2）路由模式：是防火墙的基本工作模式。在路由模式下，防火墙的各个网口设备的 IP 地址都位于不同的网段。

（3）混杂模式：指防火墙部分网口在路由模式下工作，部分网口在透明桥模式下工作。即某些子网之间以路由方式通信，而某些子网可以透明通信。

3）SNMP 配置

FG 支持 SNMP 简单网络管理协议。一方面，网络管理工具可以实时获取 FG 的状态为其提供相关的系统状态、网络接口状态、IP 状态、ARP 表状态和 SNMP 服务状态等信息。另一方面，FG为网络管理平台定期提供有关 FG 防火墙的信息，如入侵信息、管理信息和系统信息。

SNMP 的界面配置可分为 4 个部分。

（1）防火墙位置标识：对系统本地位置信息进行配置。

（2）共同体（Community）：用于简单的权限控制，默认为 fgprivate。

（3）SNMP 管理服务器地址：网络管理服务器地址。

（4）管理服务器 Trap 服务端口：网络管理服务器 Trap 接收端口，默认端口号为 162。

4）双机热备

FG 防火墙双机热备份系统是由两台配置相同的防火墙组成，采用主从工作方式。正常情况下一台处于工作状态，为主防火墙，另一台处于热备状态，为从防火墙。当主防火墙发生网络故障和硬件故障等情况时，备份防火墙可以迅速切换工作状态，代替主防火墙工作，从

而保证了整个网络的正常运行。双机热备功能适用于对系统有高可靠性要求的网络安全需求。

双机热备的硬件连接如图 7-6 所示，将防火墙的各个网口分别通过交换机或集线器用网线连接。硬件连接完成后，需要在 FireControl 控制端进行设置。只有策略管理员可以设置双机热备功能。双机热备系统只在桥和路由模式下工作，不支持混杂模式及 VLAN。

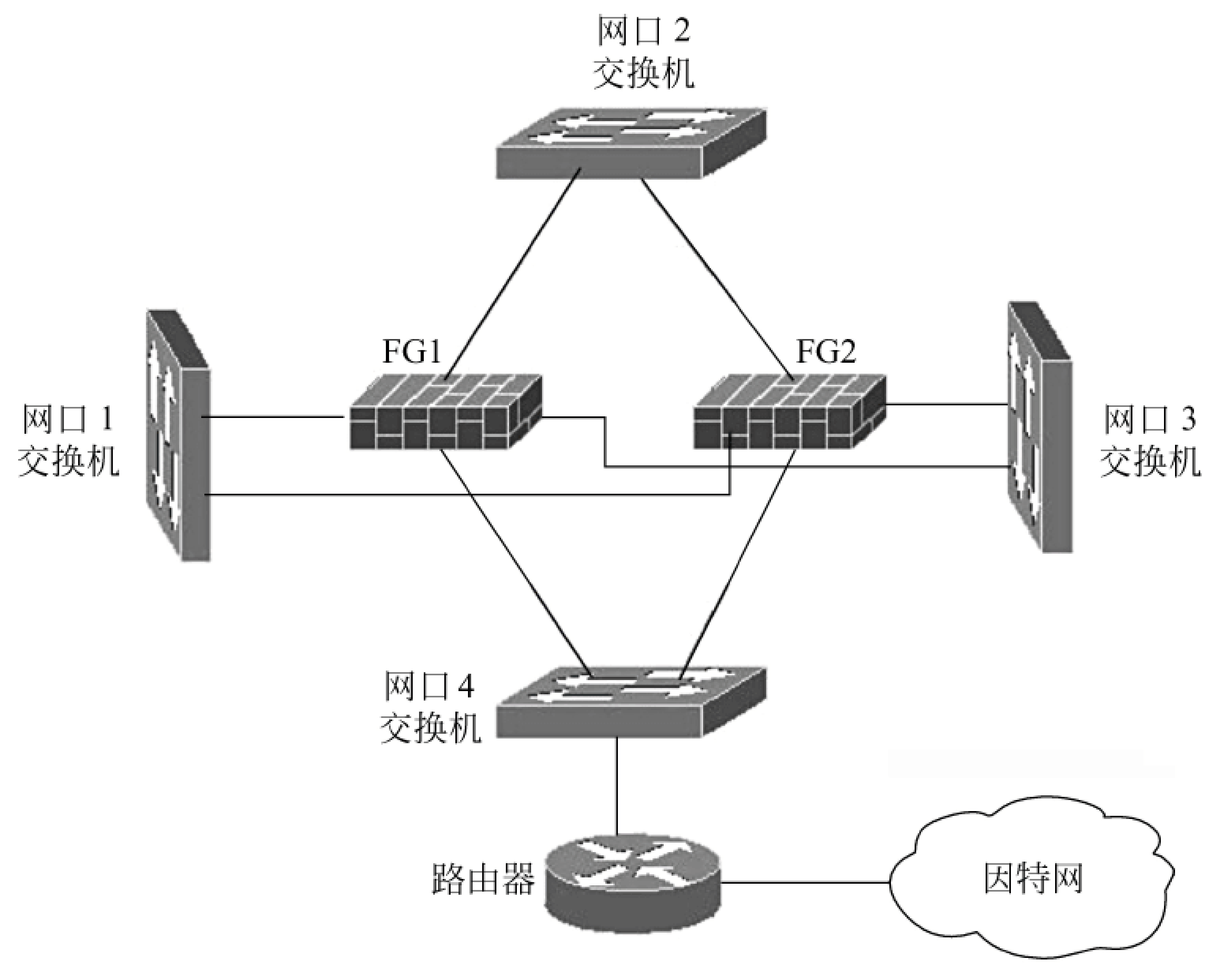


图 7-6　双机热备连机示意

3．规则配置

FG 防火墙提供基于状态检测技术的包过滤，能够根据数据包的地址、协议和端口进行访问控制。FG 防火墙包过滤功能主要是通过制订过滤规则集，对数据包头源地址、目的地址和端口号、协议类型等标志进行检查，判定是否允许通过。对于满足过滤规则的数据包，根据规则的策略决定放过或者丢弃，不满足规则的包则被丢弃。包过滤规则采用按顺序匹配的方式，即首先匹配前面的规则，若匹配则不再向下执行，因此一定要注意规则设置的顺序问题。

防火墙的规则配置是面向网口设备的，每个网口上的规则是指：这个接口设备接收到的数据包要经过这些规则的过滤，此处的接口包括物理接口设备和 VLAN 设备。每条规则详细描述了源/目的地址、目的端口、协议、数据流向、状态检测和策略等信息。

策略包括 4 种：允许（ACCEPT）、禁止（DROP）、自动封禁（AUTO）、用户认证（AUTH）。

（1）允许：接受此包。

（2）禁止：丢弃此包。

（3）自动封禁：FG启动入侵检测功能后，需要在防火墙模块相应接口设备（包括物理网口、VLAN设备）上添加一条“自动封禁”规则，才能自动封禁入侵IP。FG的每个网口都可以做自动封禁。一般情况下，如果入侵检测功能的自动封禁设置选择物理网口进行监听。

（4）用户认证：对于分配了公网IP的内部用户，如果出于安全的目的，管理员希望用户必须通过认证才能访问因特网，则需要在用户管理模块中选择一种认证方式（内置账号认证，或第三方认证），并且在防火墙模块的相应接口设备上（一般是内部网对应的网口）加一条用户认证规则。FG的每个接口设备都可以添加认证规则，包括每一个物理网口（如网口1、网口2等）和VLAN设备（如网口2.100）。

7.2.4 防火墙系统安装与配置实例

为使读者更加容易理解防火墙的概念和配置方法。下面仍以方正方御防火墙为例，在一个简单的网络环境中安装和配置防火墙。

1. 基础环境

网络安装防火墙前其拓扑结构如图7-7所示，具体环境如下。

（1）外网（即外部网）接口S1地址为211.156.169.6/30（子网掩码表示由30个1组成，下同），上连因特网接口端地址为211.156.169.5/30。

（2）内网（即内部网）接口地址有两个。

- E0：210.156.169.1/28（可用地址空间是210.156.169.1～210.156.169.14，广播地址为210.156.169.15）。
- E0：192.168.1.1/24（内部网私有地址，地址空间为192.168.1.1～192.168.1.254，广播地址为192.168.1.255）。

（3）对外服务器默认网关为210.156.169.1，内部网主机默认网关为192.168.1.1。

（4）部分外网服务器地址如下。

- WWW服务器：210.156.169.2/28。
- E-mail服务器：210.156.169.3/28。
- FTP服务器：210.156.169.4/28。
- DNS服务器：210.156.169.5/28。
- 代理服务器：210.156.169.6/28。
- Telnet服务器：210.156.169.7/28。

（5）部分内网主机地址如下。

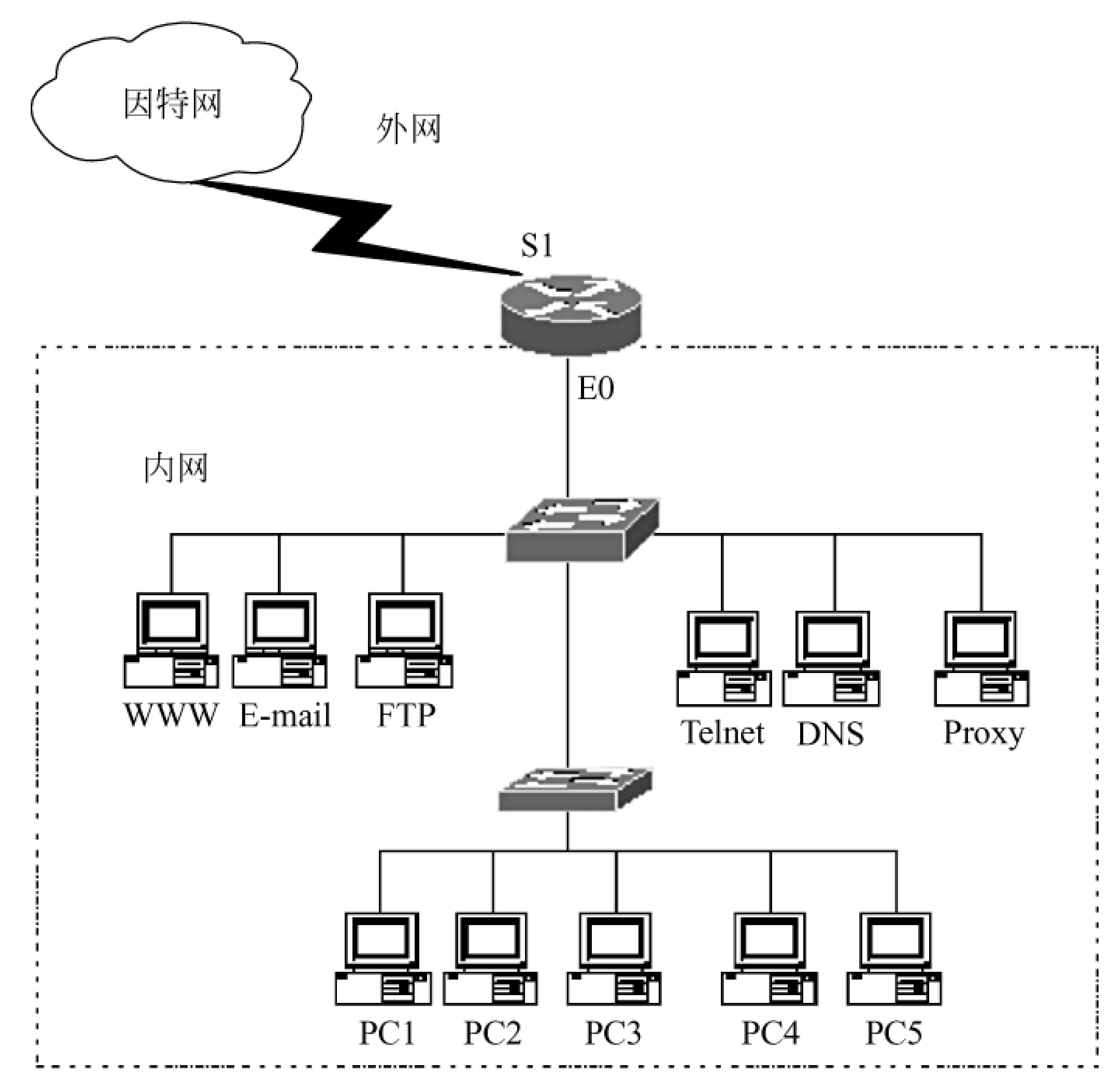


图 7-7　安装防火墙前网络拓扑结构

- PC1：192.168.1.2/24。
- PC2：192.168.1.3/24。
- PC3：192.168.1.10/24。
- PC4：192.168.1.11/24。
- PC5：192.168.1.200/24。

(6) 内部网主机通过代理服务器(210.156.169.6)上网。

2. 实施后环境

网络安装防火墙后，其拓扑结构如图 7-8 所示，具体环境如下：

(1) 防火墙工作在混杂模式；

(2) 内部主机同内部服务器系统严格分开；

(3) 内部私有地址主机，内部服务器系统，外部网络分成严格的 3 个区域(内网，外网，DMZ 区域)；

(4) 内网网口对应防火墙上网口 1，外网网口对应防火墙上网口 2，DMZ 区域对应防火墙网口 3(网口 4 未使用，如果用户购买的是 3 端口防火墙，则无网口 4)；

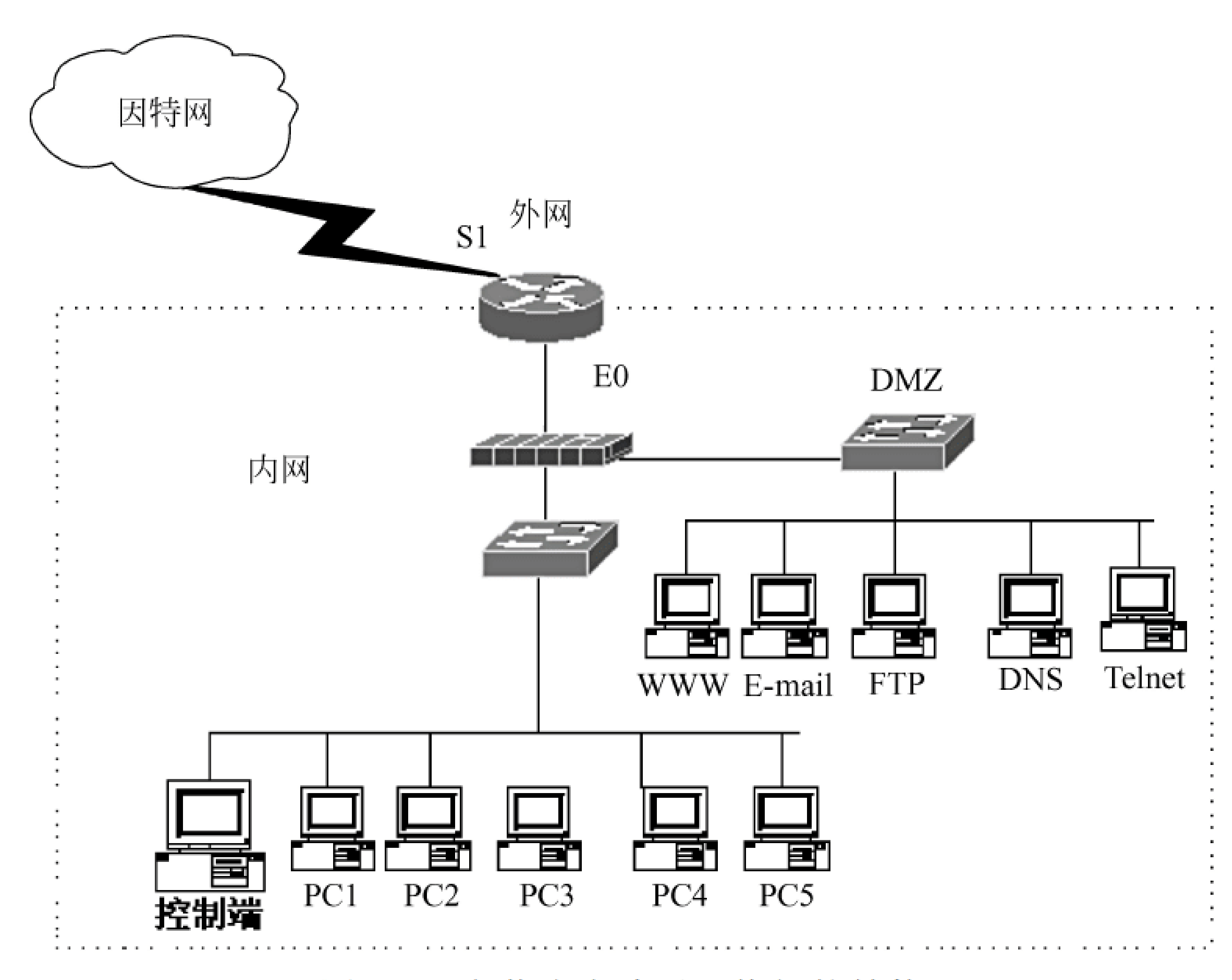


图 7-8　安装防火墙后网络拓扑结构

（5）在各个区域之间实施严格的访问控制，保障系统安全；

（6）内部服务器系统采用公有地址，内部网访问外部网通过 NAT 实现，取代以前的代理服务器系统；

（7）将防火墙控制端放置在内部网；

（8）控制端地址为 192.168.1.7/24；

（9）路由器上将取消 E0 的第 2 个地址 192.168.1.1/24。

3. 配置策略

1）基本配置

（1）网口 1 设为防火墙内部网接口和管理口，地址 192.168.1.1，设置好相应的子网掩码后将其选为控制口，然后提交系统，使设备配置生效，如图 7-9 所示。

（2）将 DMZ 区域和外网区域设置为桥，同时在桥上绑定 IP 地址 210.156.169.6/28（为原代理服务器地址），配置完后提交系统，使设备配置生效，如图 7-10 所示。

（3）添加内部网、DMZ 区域以及外部网各设备别名，如图 7-11 所示。

2）规则配置

（1）按照实际情况配置各种安全措施，如内部网访问 DMZ 区域 WWW 服务器规则，内部网访问 DMZ 区域 Telnet 服务器规则等，如图 7-12 所示。



图 7-9　网口 1 配置

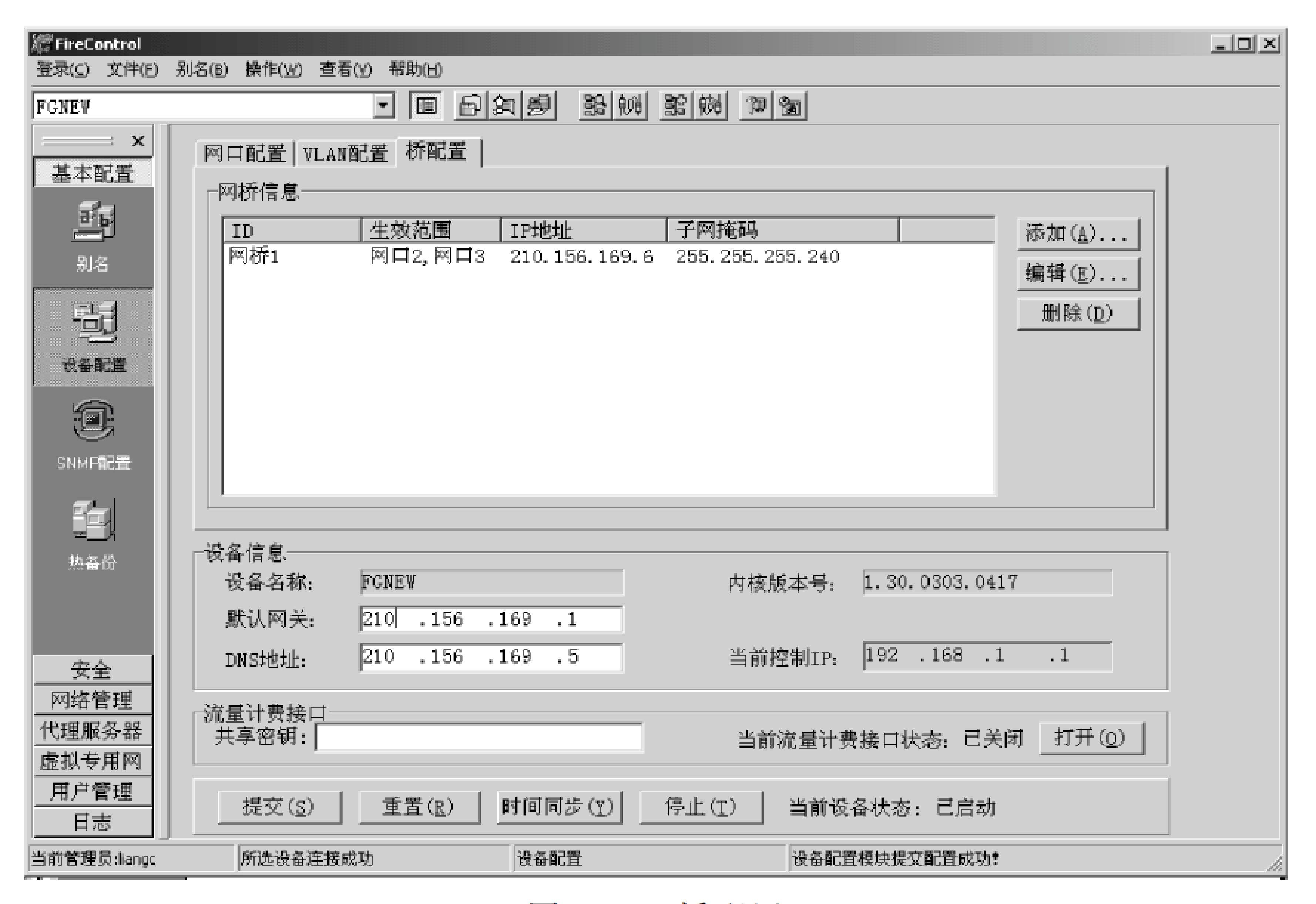


图 7-10　桥配置

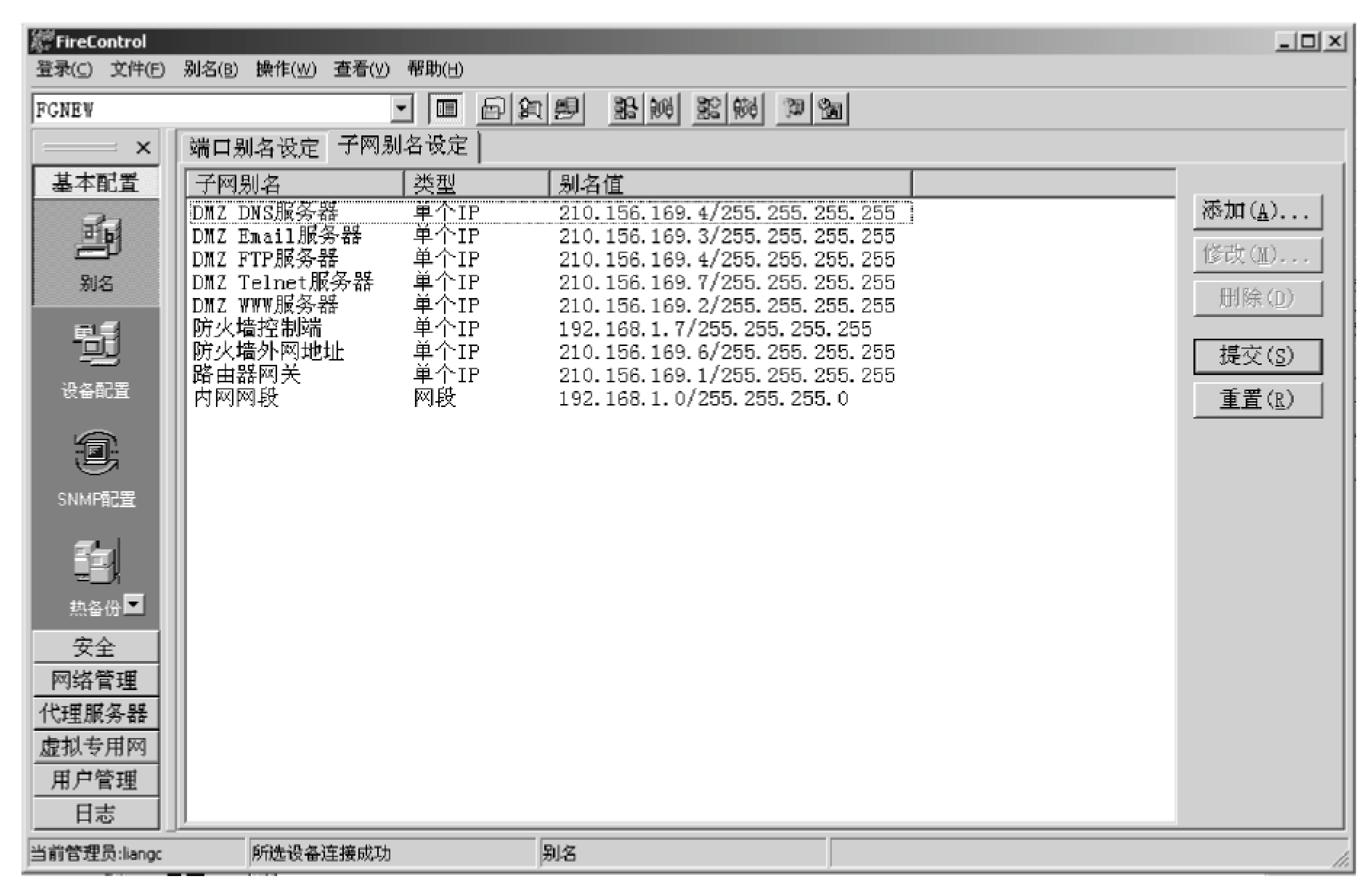


图 7-11　配置设备别名

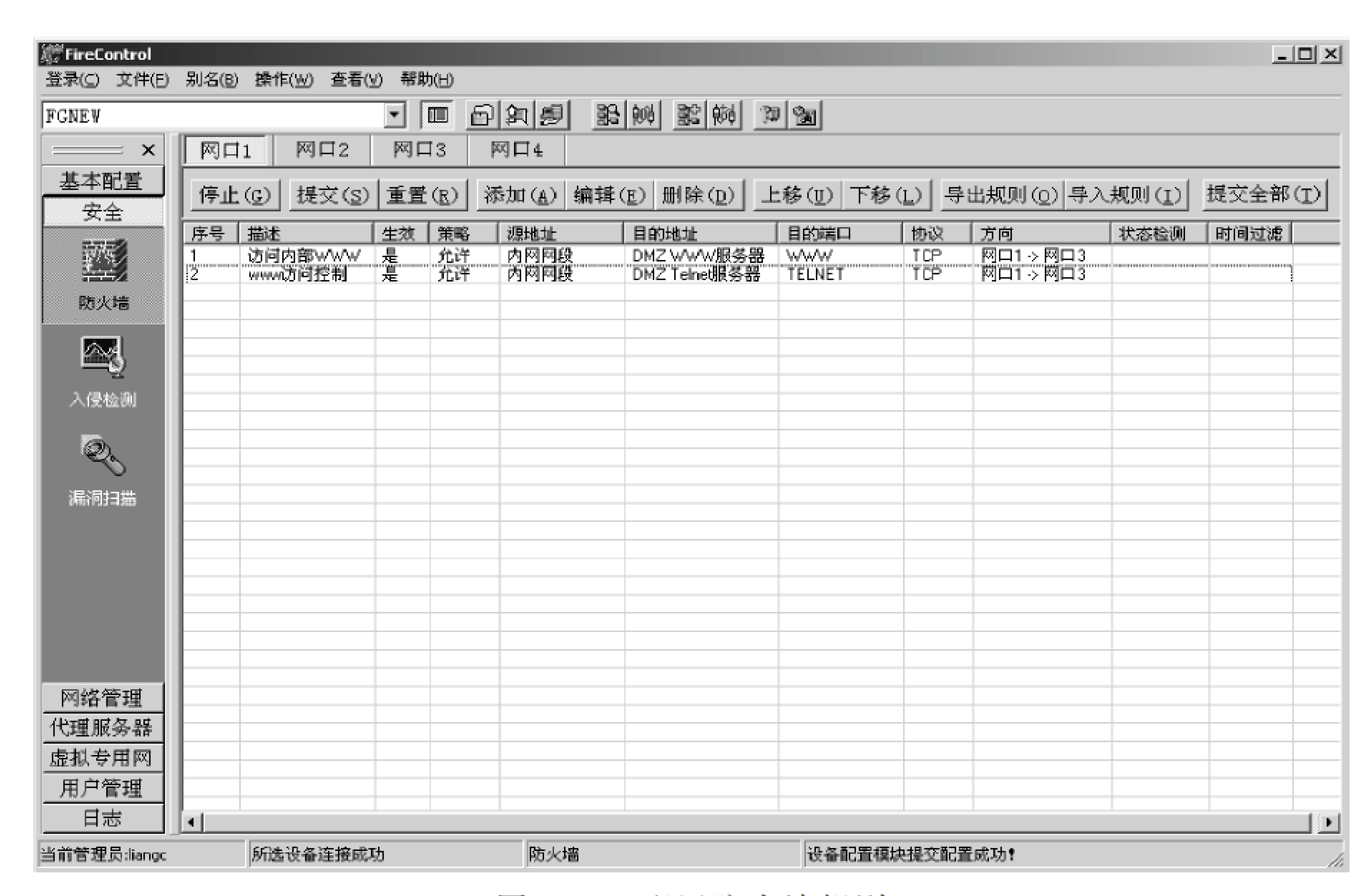
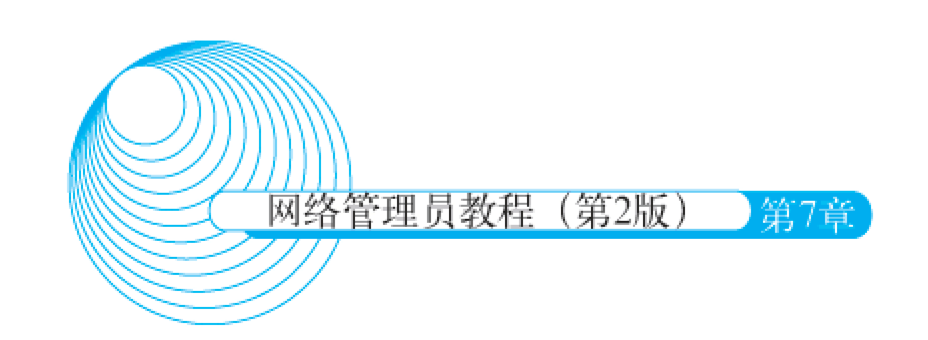


图 7-12　配置防火墙规则



（2）NAT 规则设置。在原系统中，内部网通过代理服务器 210.156.169.6 上网。调整后，内部网的网络用户可以直接上网，不需要代理服务器。在防火墙上设置 NAT 功能实现地址转换：内部网访问外部 WWW 时，全部将内部地址转换成防火墙外部网地址 210.156.169.6。如图 7-13 所示。

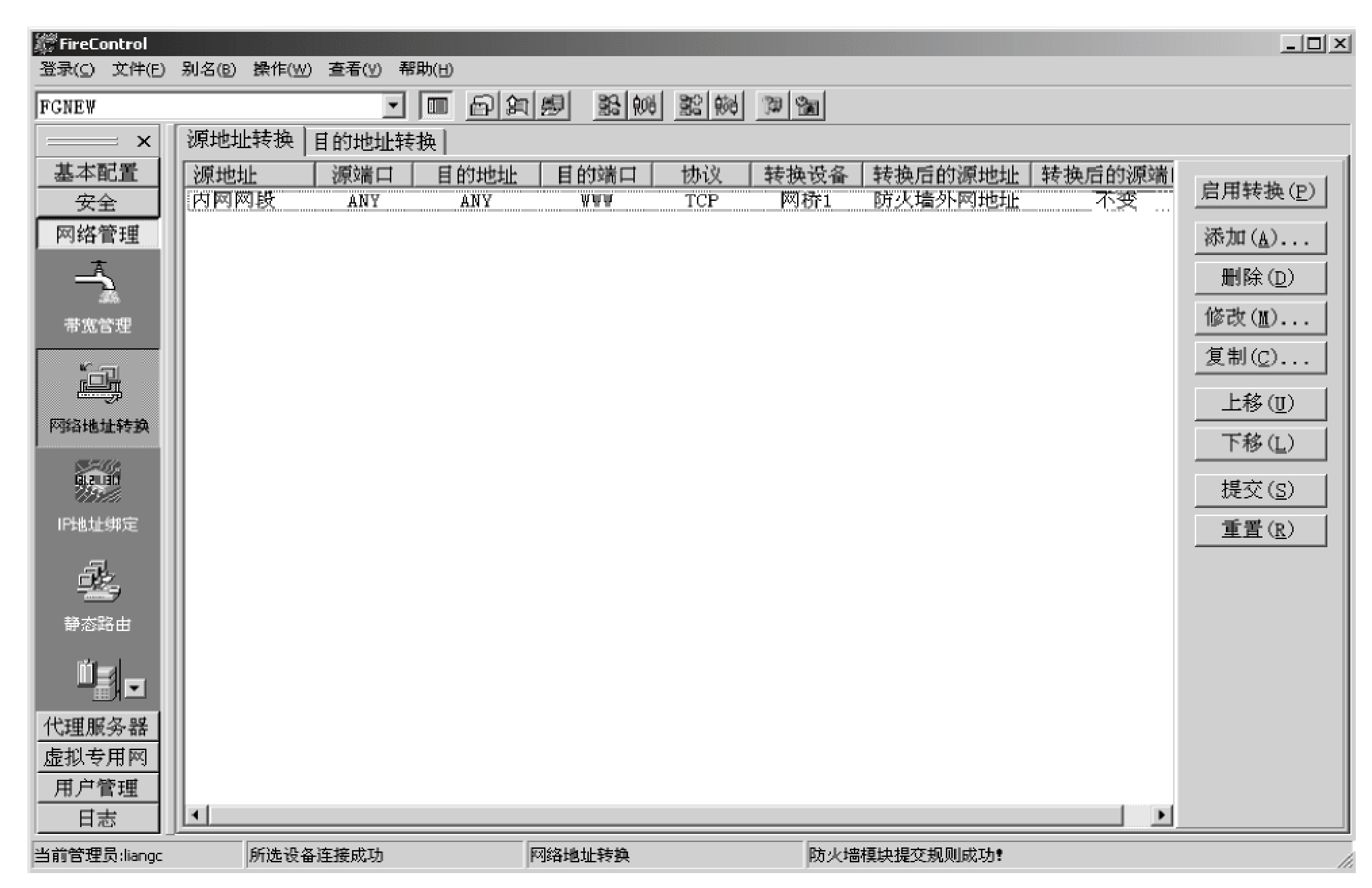


图 7-13　配置 NAT 规则

7.3　入侵检测

7.3.1　入侵检测系统简介

1. 入侵检测系统概念

当越来越多的公司将其核心业务向因特网转移的时候，网络安全作为一个无法回避的问题呈现在人们面前。传统的网络安全系统一般采用防火墙作为安全的第一道防线。而随着攻击者网络知识的日趋成熟，攻击工具与手法的日趋复杂多样，单纯的防火墙策略已经无法满足对安全高度敏感的部门的需要，网络的防卫必须采用一种纵深的、多样的手段。与此同时，当今的网络环境也变得越来越复杂，各式各样的复杂设备需要不断地升级、补漏，这使得网络管理员的

工作不断加重，一些不经意的疏忽便有可能造成安全的重大隐患。在这种环境下，入侵检测系统成为了安全市场上新的热点，不仅愈来愈多地受到人们的关注，而且已经开始在各种不同的环境中发挥其关键作用。

入侵检测是一种主动保护自己免受攻击的网络安全技术。作为防火墙的合理补充，入侵检测技术能够帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、攻击识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测。

“入侵”(Intrusion)是个广义的概念，不仅包括被发起攻击的人（如恶意的黑客）取得超出合法范围的系统控制权，也包括收集漏洞信息、拒绝服务（Denial of Service）等对计算机系统造成危害的行为。入侵检测（Intrusion Detection），顾名思义，便是对入侵行为的发觉。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统（IDS，Intrusion Detection System）。与其他安全产品不同的是，入侵检测系统需要更多的智能，它必须能够对得到的数据进行分析，并得出有用的结果。一个合格的入侵检测系统能大大简化管理员的工作，保证网络安全的运行。

2. 入侵检测系统的功能

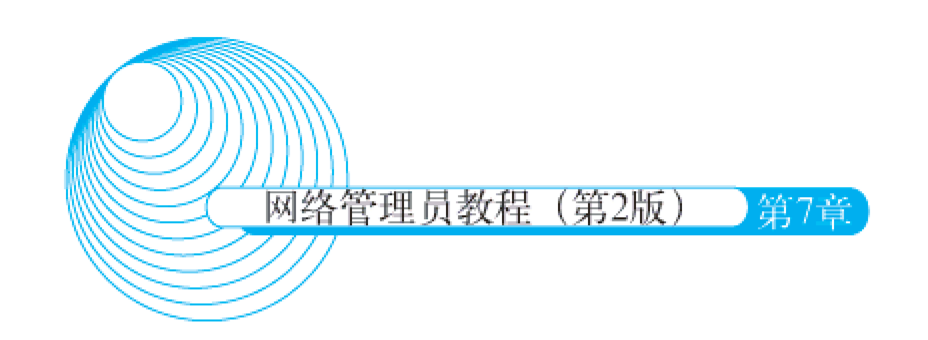
由于入侵检测系统的市场在近几年中飞速发展，许多公司相继投入到这一领域上来。有的作为独立的产品，有的作为防火墙的一部分，其结构和功能也不尽相同。通常来说，入侵检测系统均应包括以下一些主要功能：

(1) 监测并分析用户和系统的活动；
(2) 核查系统配置和漏洞；
(3) 评估系统关键资源和数据文件的完整性；
(4) 识别已知的攻击行为；
(5) 统计分析异常行为；
(6) 操作系统日志管理，并识别违反安全策略的用户活动。

3. 入侵检测系统分类

一般来说，入侵检测系统可分为主机型和网络型。在实际使用时，也可将二者结合使用。

主机型入侵检测系统往往以系统日志、应用程序日志等作为数据源，当然也可以通过其他手段（如监督系统调用）从所在的主机收集信息并进行分析。主机型入侵检测系统保护的一般是所在的系统。主机型 IDS 的优点是：系统的内在结构没有任何束缚，同时可以利用操作系统



本身提供的功能、并结合异常分析，更准确地报告攻击行为。它的缺点是：必须为不同的平台开发不同的程序，增加了系统负荷。

网络型入侵检测系统的数据源则是网络上的数据包。通常将一台主机的网卡设为混杂模式，监听所有本网段内的数据包并进行判断。一般网络型入侵检测系统担负着保护整个网段的任务。网络型 IDS 的优点主要是简便，一个网段上只须安装一个或几个这样的系统，便可以监测整个网段的情况。同时，由于往往使用单独的计算机做这种应用，不会给运行关键业务的主机带来负载上的增加。它的缺点是：由于现在网络的结构日趋复杂，以及高速网络的普及，这种结构已逐渐显示出其局限性。

4. 入侵检测系统的组成及部署

一般来说入侵检测系统由 3 部分组成，分别是事件产生器、事件分析器和响应单元。通常，这 3 部分分别运行在 3 台独立的主机上。对于 IDS 而言，事件产生器所在的位置是十分重要的，因为它决定了“事件”的可见度。

对于主机型 IDS，其事件产生器位于其所监测的主机上。

对于网络型 IDS，其事件产生器的位置有多种可能。如果网段用总线式的集线器相连，则可将其简单地接在集线器的一个端口上。对于交换式以太网交换机，问题则会变得复杂。由于交换机不采用共享媒质的办法，传统的采用一个 sniffer 来监听整个子网的办法则不再可行。解决的办法有：

(1) 交换机的核心芯片上一般有一个用于调试的端口(span port)，任何其他端口的进出信息都可从此得到。如果交换机厂商把此端口开放出来，用户可将 IDS 系统接到此端口上。这种方法的优点是无须改变 IDS 体系结构，缺点是采用此端口会降低交换机性能。

(2) 把入侵检测系统放在交换机内部或防火墙内部等数据流的关键出入口。这种方法的优点是可以得到几乎所有的关键数据，缺点是必须与其他厂商紧密合作，并且会降低网络性能。

(3) 采用分接器(Tap)，将其接在所有要监测的线路上。这种方法的优点是在不降低网络性能的前提下收集了所需的信息，缺点是必须购买额外的设备(Tap)。

5. 入侵检测技术分类

对各种事件进行分析，从中发现违反安全策略的行为是入侵检测系统的核心功能。从技术上，入侵检测分为两种：一种基于标识(signature-based)，另一种基于异常情况(anomaly-based)。

对于基于标识的检测技术来说，首先要定义违背安全策略的事件的特征，如网络数据包的某些头信息。检测主要就是判别在所收集到的数据中是否出现了这类特征。此方法非常类似杀毒软件。

而基于异常的检测技术则是先定义一组系统“正常”情况的数值，如 CPU 利用率、内存利用

率、文件校验和等(这类数据可以人为定义,也可以通过观察系统、并用统计的办法得出),然后将系统运行时的数值与所定义的“正常”情况比较,得出是否有被攻击的迹象。这种检测方式的核心在于如何定义所谓的“正常”情况。

以上两种检测技术的方法、所得出的结论有非常大的差异。基于异常的检测技术的核心是维护一个知识库。对于已知的攻击,它可以详细、准确地报告出攻击类型,但是对未知攻击却效果有限,而且知识库必须不断更新。基于异常的检测技术则无法准确判别出攻击的手法,但它可以(至少在理论上可以)判别更广泛、甚至未发觉的攻击。如果条件允许,两者结合的检测会达到更好的效果。

6. 入侵检测系统通信协议

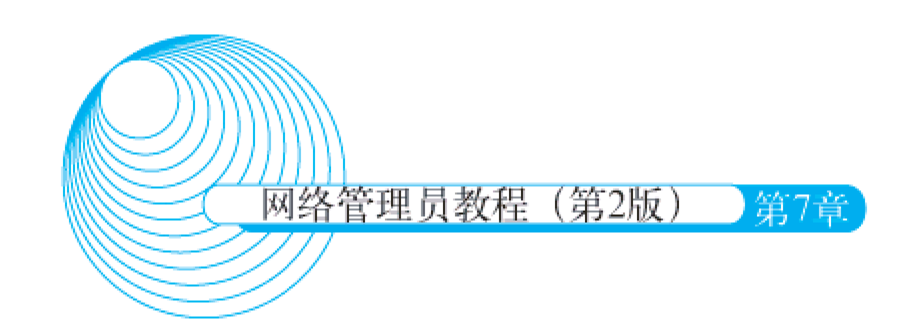
IDS系统组件之间需要通信,不同厂商的IDS系统之间也需要通信。如何保证分析系统与控制系统之间传输信息的真实性和完整性,怎样对通信的双方进行身份验证和保密传输,怎样防止主动和被动攻击,如何在系统异常中断时正常工作,等等。所有这些均说明:定义统一的协议,使各部分能够根据协议所制订的标准进行沟通是十分必要的。

IETF目前有一个专门的小组IDWG(Intrusion Detection Working Group)负责定义这种通信格式,称作IDEF(Intrusion Detection Exchange Format)。目前只有相关的草案,并未形成正式的RFC文档。尽管如此,草案为IDS各部分之间甚至不同IDS系统之间的通信提供了一定的指引。另外,IAP(Intrusion Alert Protocol)是IDWG制订的、运行于TCP之上的应用层协议,其设计在很大程度上参考了HTTP,并且补充了许多其他功能(如可从任意端发起连接,结合了加密、身份验证等)。

7.3.2 入侵检测系统基本原理

1. 信息收集

入侵检测的基础是信息收集,内容包括系统、网络、数据及用户活动的状态和行为。而且,需要在计算机网络系统中的若干不同关键点(不同网段和不同主机)收集信息,尽可能扩大检测范围。当然,入侵检测很大程度上依赖于收集信息的可靠性和正确性,因此,很有必要只利用所知道的真正的和精确的软件来报告这些信息。因为黑客经常替换软件以搞混和移走这些信息,例如替换被程序调用的子程序、库和其他工具。黑客对系统的修改可能使系统功能失常但表面上看起来跟正常的一样。例如,UNIX系统的PS指令可以被替换为一个不显示侵入过程的指令,或者是编辑器被替换成一个读取不同于指定文件的文件。这需要保证用来检测网络系统的软件的完整性,特别是入侵检测系统软件本身应具有相当强的坚固性,防止被篡改而收集到错误的信息。入侵检测利用的信息一般来自以下4个方面:



1）系统和网络日志文件

黑客经常在系统日志文件中留下他们的踪迹，因此，充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据，这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快地启动相应的应急响应程序。日志文件中记录了各种行为类型，每种类型又包含不同的信息，例如记录“用户活动”类型的日志，就包含登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。很显然地，对用户活动来讲，不正常的或不期望的行为就是重复登录失败、登录到不期望的位置以及非授权的企图访问重要文件等。

2）目录和文件中的不期望的改变

网络环境中的文件系统包含了很多软件和数据文件，其中包含有重要信息的文件和私有数据文件经常是黑客修改或破坏的目标。目录和文件中的不期望的改变（包括修改、创建和删除），特别是那些正常情况下限制访问的，很可能就是一种入侵产生的指示和信号。黑客经常替换、修改和破坏他们获得访问权限系统上的文件，同时为了隐藏他们的表现及活动痕迹，又都会尽力去替换系统程序或修改系统日志文件。

3）程序执行中的不期望行为

网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和特定目的的应用，例如数据库服务器。每个在系统上执行的程序由一到多个进程来实现。每个进程执行在具有不同权限的环境中，这种环境控制着进程可以访问的系统资源、程序和数据文件等。一个进程的执行行为由它运行时执行的操作来表现，操作执行的方式不同，它利用的系统资源也就不同。操作包括计算、文件传输、设备和其他进程，以及与网络间其他进程的通信。一个进程出现了不期望的行为可能表明黑客正在入侵系统。黑客可能会将程序或服务的运行分解，从而导致程序以非管理员意图的方式操作。

4）物理形式的入侵信息

包括两个方面的内容，一是未授权的对网络硬件的连接；二是对物理资源的未授权访问。黑客会想方设法去突破网络的周边防卫，如果他们能够在物理上访问内部网，就能安装他们自己的设备和软件。由此，黑客就可以知道网上的由用户加上去的不安全（未授权）设备，然后利用这些设备访问网络。例如，用户在家里可能安装 Modem 以访问远程办公室，与此同时黑客正在利用自动工具来识别在公共电话线上的 Modem，如果拨号访问流量经过了这些自动工具，那么这一个拨号访问就成为了威胁网络安全的后门。黑客就会利用这个后门来访问内部网，从而越过了内部网原有的防护措施，然后捕获网络流量，进而攻击其他系统，并偷取敏感的私有信息等。

2. 信号分析

入侵检测的核心是信号分析。针对上述 4 类收集到的有关系统、网络、数据及用户活动的

状态和行为的信息，一般通过3种技术手段进行分析：模式匹配，统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

1）模式匹配

模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该过程可以很简单（如通过字符串匹配来寻找一个简单的条目或指令），也可以很复杂（如利用正规的数学表达式来表示安全状态的变化）。一般来讲，一种进攻模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。该方法的一大优点是只须收集相关的数据集合，这样可以显著减少系统负担，且该技术已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是，该方法存在的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

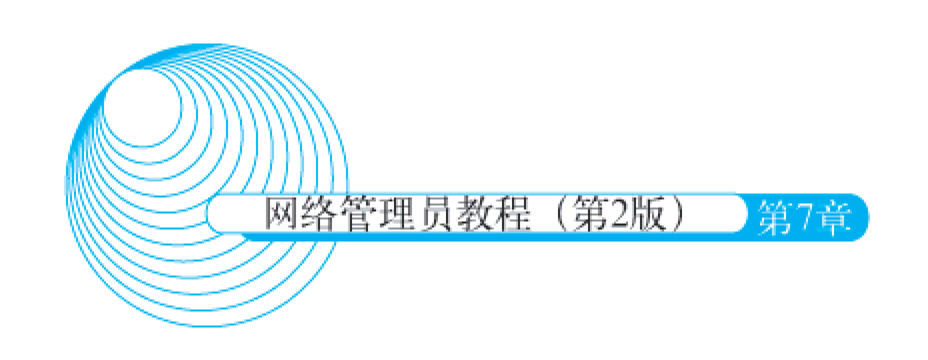
2）统计分析

统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。测量属性的平均值将被用来与网络、系统的行为进行比较，当观察值在正常值范围之外时，就认为有入侵发生。例如，统计分析可能标识一个不正常行为，因为它发现一个在晚上8点至早上6点不登录的账户却在凌晨2点试图登录。其优点是可检测到未知的入侵和更为复杂的入侵，缺点是误报、漏报率高，且对用户正常行为的突然改变不适应。具体的统计分析方法如基于专家系统的、基于模型推理的和基于神经网络的分析方法，目前正处于研究热点和迅速发展之中。

3）完整性分析

完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性，它在发现被更改以及被特洛伊化的应用程序方面特别有效。完整性分析利用强有力的加密机制，称为消息摘要函数（如MD5），它能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能够发现。缺点是一般以批处理方式实现，不用于实时响应。尽管如此，完整性检测方法还应该是网络安全产品的必要手段之一。例如，可以在每一天的某个特定时间内开启完整性分析模块，对网络系统进行全面的扫描检查。

入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵，从立体纵深、多层次防御的角度对系统实施保护。在国内，随着上网的关键部门、关键业务越来越多，迫切需要具有自主版权的入侵检测产品。但现状是入侵检测仅仅停留在研究和实验样品（缺乏升级和服务）阶段，或者是防火墙中集成一些较为初级的入侵检测模块。可见，入侵检测产品仍具有较大的发展空间，从技术途径来讲，除了完善常规的、传统的技术（模式识别和完整性检测）外，应重点加强统计分析的相关技术研究。



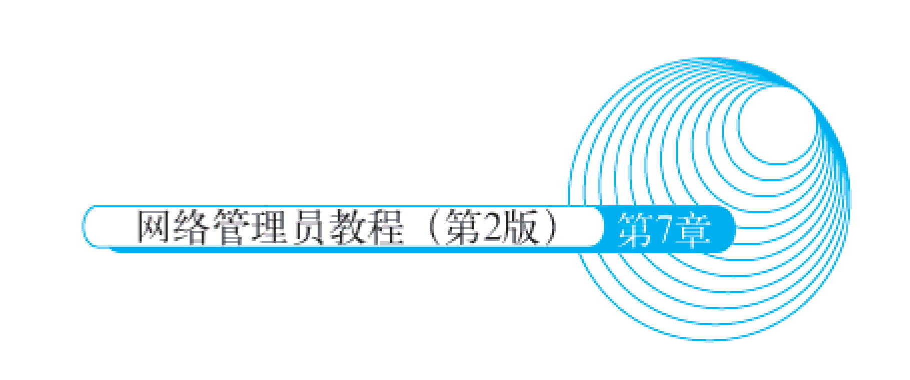
7.3.3 入侵防护系统

随着网络入侵事件的不断增加和黑客攻击水平的不断提高，一方面企业网络感染病毒、遭受攻击的频率日益加快，另一方面企业网络受到攻击作出响应的时间却越来越滞后。解决这一矛盾，传统的防火墙或入侵检测技术(IDS)已显得力不从心，这就需要引入一种全新的技术——入侵防护系统(IPS，Intrusion Prevention System)。

1. IPS 简介

防火墙是实施访问控制策略的系统，对流经的网络流量进行检查，拦截不符合安全策略的数据包。入侵检测技术(IDS)通过监视网络或系统资源，寻找违反安全策略的行为或攻击迹象，并发出报警。传统的防火墙旨在拒绝那些明显可疑的网络流量，但仍然允许某些流量通过，因此防火墙对于很多入侵攻击仍然无计可施。绝大多数 IDS 系统都是被动的，而不是主动的。也就是说，在攻击实际发生之前，它们往往无法预先发出警报。而入侵防护系统 (IPS) 则倾向于提供主动防护，其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。IPS 是通过直接嵌入到网络流量中实现这一功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，有问题的数据包，以及所有来自同一数据流的后续数据包，都能在 IPS 设备中被清除掉。

IPS 实现实时检查和阻止入侵的原理在于 IPS 拥有数目众多的过滤器，能够防止各种攻击。当新的攻击手段被发现之后，IPS 就会创建一个新的过滤器。IPS 数据包处理引擎是专业化定制的集成电路，可以深层检查数据包的内容。如果有攻击者利用 Layer 2 (介质访问控制)至 Layer 7(应用)的漏洞发起攻击，IPS 能够从数据流中检查出这些攻击并加以阻止。传统的防火墙只能对 Layer 3 或 Layer 4 进行检查，不能检测应用层的内容。防火墙的包过滤技术不会针对每一字节进行检查，因而也就无法发现攻击活动，而 IPS 可以做到逐一字节地检查数据包。所有流经 IPS 的数据包都被分类，分类的依据是数据包中的报头信息，如源 IP 地址和目的 IP 地址、端口号和应用域。每种过滤器负责分析相对应的数据包。通过检查的数据包可以继续前进，包含恶意内容的数据包就会被丢弃，被怀疑的数据包需要接受进一步的检查。针对不同的攻击行为，IPS 需要不同的过滤器。每种过滤器都设有相应的过滤规则，为了确保准确性，这些规则的定义非常广泛。在对传输内容进行分类时，过滤引擎还需要参照数据包的信息参数，并将其解析至一个有意义的域中进行上下文分析，以提高过滤的准确性。过滤器引擎集合了流水和大规模并行处理硬件，能够同时执行数千次的数据包过滤检查。并行过滤处理可以确保数据包能够不间断地快速通过系统，不会对速度造成影响。这种硬件加速技术对于 IPS 具有重要意义，因为传统的软件解决方案必须串行进行过滤检查，会导致系统性能大打折扣。



2. IPS 的种类

1）基于主机的入侵防护（HIPS）

HIPS 通过在主机/服务器上安装软件代理程序，防止网络攻击入侵操作系统以及应用程序。基于主机的入侵防护能够保护服务器的安全弱点不被不法分子所利用。Cisco 公司的 Okena、NAI 公司的 McAfee Entercept、冠群金辰的龙渊服务器核心防护都属于这类产品，因此它们在防范红色代码和 Nimda 的攻击中，起到了很好的防护作用。基于主机的入侵防护技术可以根据自定义的安全策略以及分析学习机制来阻断对服务器、主机发起的恶意入侵。HIPS 可以阻断缓冲区溢出、改变登录口令、改写动态链接库以及其他试图从操作系统夺取控制权的入侵行为，整体提升主机的安全水平。在技术上，HIPS 采用独特的服务器保护途径，利用由包过滤、状态包检测和实时入侵检测组成分层防护体系。这种体系能够在提供合理吞吐率的前提下，最大限度地保护服务器的敏感内容，它既可以软件形式嵌入到应用程序对操作系统的调用当中，通过拦截针对操作系统的可疑调用，提供对主机的安全防护；也可以更改操作系统内核程序的方式，提供比操作系统更加严谨的安全控制机制。由于 HIPS 工作在受保护的主机/服务器上，它不但能够利用特征和行为规则检测，阻止诸如缓冲区溢出之类的已知攻击，还能够防范未知攻击，防止针对 Web 页面、应用和资源的未授权的任何非法访问。HIPS 与具体的主机/服务器操作系统平台紧密相关，不同的平台需要不同的软件代理程序。

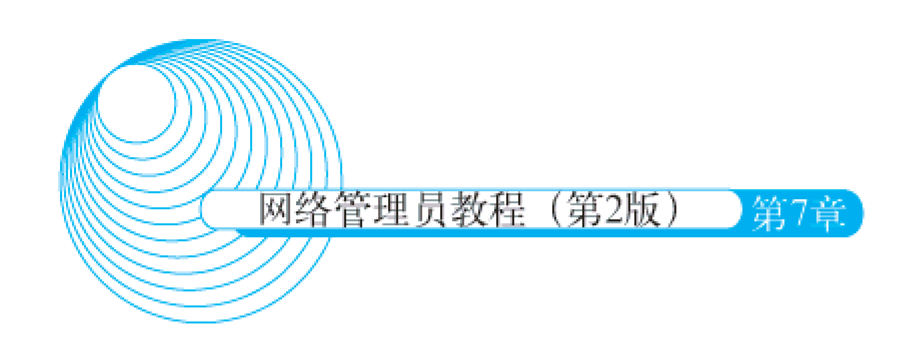
2）基于网络的入侵防护（NIPS）

NIPS 通过检测流经的网络流量，提供对网络系统的安全保护。由于它采用在线连接方式，所以一旦辨识出入侵行为，NIPS 就可以去除整个网络会话，而不仅仅是复位会话。同样由于实时在线，NIPS 需要具备很高的性能，以免成为网络的瓶颈，因此 NIPS 通常被设计成类似于交换机的网络设备，提供线速吞吐速率以及多个网络端口。

NIPS 必须基于特定的硬件平台，才能实现千兆级网络流量的深度数据包检测和阻断功能。这种特定的硬件平台通常可以分为 3 类：网络处理器（网络芯片）、专用的 FPGA 编程芯片、专用的 ASIC 芯片。

在技术上，NIPS 吸取了目前 NIDS 的所有成熟技术，包括特征匹配、协议分析和异常检测。特征匹配是最广泛应用的技术，具有准确率高、速度快的特点。基于状态的特征匹配不但可以检测攻击行为的特征，还能检查当前网络的会话状态，避免受到欺骗攻击。

协议分析是一种较新的入侵检测技术，它充分利用网络协议的高度有序性，并结合高速数据包捕捉和协议分析，来快速检测某种攻击特征。协议分析正在逐渐进入成熟应用阶段。协议分析能够理解不同协议的工作原理，以此分析这些协议的数据包，来寻找可疑或不正常的访问行为。协议分析不仅仅基于协议标准（如 RFC），还基于协议的具体实现，这是因为很多协议的实现偏离了协议标准。通过协议分析，IPS 能够针对插入（Insertion）与规避（Evasion）攻击进行



检测。异常检测的误报率比较高，NIPS不将其作为主要技术。

3）应用入侵防护（AIP）

NIPS产品有一个特例，即应用入侵防护（AIP，Application Intrusion Prevention），它把基于主机的入侵防护扩展成为位于应用服务器之前的网络设备。AIP被设计成一种高性能的设备，配置在应用数据的网络链路上，以确保用户遵守设定好的安全策略，保护服务器的安全。NIPS工作在网络上，直接对数据包进行检测和阻断，与具体的主机/服务器操作系统平台无关。

NIPS的实时检测与阻断功能很有可能出现在未来的交换机上。随着处理器性能的提高，每一层次的交换机都有可能集成入侵防护功能。

3. IPS技术特征

（1）嵌入式运行：只有以嵌入模式运行的IPS设备才能够实现实时的安全防护，实时阻拦所有可疑的数据包，并对该数据流的剩余部分进行拦截。

（2）深入分析和控制：IPS必须具有深入分析能力，以确定哪些恶意流量已经被拦截，根据攻击类型、策略等来确定哪些流量应该被拦截。

（3）入侵特征库：高质量的入侵特征库是IPS高效运行的必要条件，IPS还应该定期升级入侵特征库，并快速应用到所有传感器。

（4）高效处理能力：IPS必须具有高效处理数据包的能力，对整个网络性能的影响保持在最低水平。

4. IPS面临的挑战

IPS技术需要面对很多挑战，其中主要有3点：单点故障、性能瓶颈、误报和漏报。

设计要求IPS必须以嵌入模式工作在网络中，而这就可能造成瓶颈问题或单点故障。如果IDS出现故障，最坏的情况也就是造成某些攻击无法被检测到，而嵌入式的IPS设备出现问题，就会严重影响网络的正常运转。如果IPS出现故障而关闭，用户就会面对一个由IPS造成的拒绝服务问题，所有客户都将无法访问企业网络提供的应用。

即使IPS设备不出现故障，它仍然是一个潜在的网络瓶颈，不仅会增加滞后时间，而且会降低网络的效率，IPS必须与数千兆或者更大容量的网络流量保持同步，尤其是当加载了数量庞大的检测特征库时，设计不够完善的IPS嵌入设备无法支持这种响应速度。绝大多数高端IPS产品供应商都通过使用自定义硬件（FPGA、网络处理器和ASIC芯片）来提高IPS的运行效率。

误报率和漏报率也需要IPS认真面对。在繁忙的网络当中，如果以每秒需要处理十条警报信息来计算，IPS每小时至少需要处理36 000条警报，一天就是864 000条。一旦生成了警报，最基本的要求就是IPS能够对警报进行有效处理。如果入侵特征编写得不是十分完善，那么“误报”就有了可乘之机，导致合法流量也有可能被意外拦截。对于实时在线的IPS来说，一旦

拦截了“攻击性”数据包，就会对来自可疑攻击者的所有数据流进行拦截。如果触发了误报警报的流量恰好是某个客户订单的一部分，其结果可想而知，这个客户整个会话就会被关闭，而且此后该客户所有重新连接到企业网络的合法访问都会被IPS拦截。

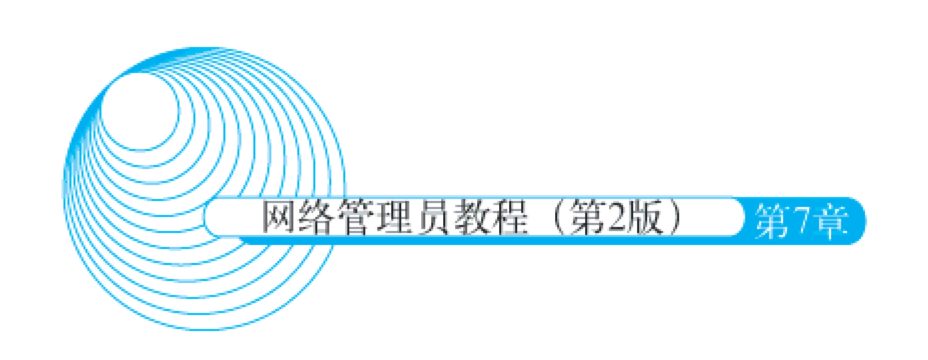
7.4 漏洞扫描

7.4.1 漏洞扫描系统简介

网络系统的安全性取决于网络系统中最薄弱的环节。然而策略的制订和实施在实际应用中相差甚远，网络系统的安全性是一个动态的过程。系统配置的不断更改，Hacker技术的不断提高，网络系统的安全系数也会不断的变化。如何及时发现网络系统中最薄弱环节？如何最大限度地保证网络系统的安全？最有效的方式就是定期对网络系统进行安全性分析，及时发现并查找漏洞并进行修改。

漏洞扫描系统是一种自动检测远程或本地主机安全性弱点的程序。通过使用漏洞扫描系统，系统管理员能够发现所维护的Web服务器的各种TCP端口的分配、提供的服务、Web服务软件版本和这些服务及软件呈现在因特网上的安全漏洞。从而在计算机网络系统安全保卫战中做到“有的放矢”，及时修补漏洞，构筑坚固的安全长城。漏洞扫描系统，因其可预知主体受攻击的可能性和具体的指证将要发生的行为和产生的后果，而受到网络安全业界的重视。这一技术的应用可以帮助识别检测对象的系统资源，分析这一资源被攻击的可能指数，了解支撑系统本身的脆弱性，评估所有存在的安全风险。

漏洞扫描技术是检测远程或本地系统安全脆弱性的一种安全技术。通过与目标主机TCP/IP端口建立连接并请求某些服务(如TELNET、FTP等)，记录目标主机的应答，搜集目标主机相关信息(如匿名用户是否可以登录等)，从而发现目标主机某些内在的安全弱点。漏洞扫描技术的重要性在于它把那些极为烦琐的安全检测，通过程序来自动完成，这不仅减轻了管理者的工作，而且缩短了检测时间，使问题发现更快。当然，也可以认为扫描技术是一种网络安全性评估技术。一般而言，扫描技术可以快速、深入地对网络或目标主机进行评估。漏洞扫描是对系统脆弱性的分析评估，能够检查、分析网络范围内的设备、网络服务、操作系统、数据库等系统的安全性，从而为提高网络安全的等级提供决策的支持。系统管理员利用漏洞扫描技术对局域网络、Web站点、主机操作系统、系统服务以及防火墙系统的安全漏洞进行扫描，可以了解在运行的网络系统中存在的不安全的网络服务，在操作系统上存在的可能导致黑客攻击的安全漏洞，还可以检测主机系统中是否被安装了窃听程序，防火墙系统是否存在安全漏洞和配置错误等。网络管理员可以利用安全扫描软件，及时发现网络漏洞并在网络攻击者扫描和利用之前予以修补，从而提高网络的安全性。



7.4.2 漏洞扫描系统基本原理

漏洞扫描系统的工作原理是：当用户通过控制平台发出了扫描命令之后，控制平台即向扫描模块发出相应的扫描请求，扫描模块在接到请求之后立即启动相应的子功能模块，对被扫描主机进行扫描。通过对从被扫描主机返回的信息进行分析判断，扫描模块将扫描结果返回给控制平台，再由控制平台最终呈现给用户。

网络漏洞扫描系统通过远程检测目标主机TCP/IP不同端口的服务，记录目标给予的回答。通过这种方法，可以搜集到很多目标主机的各种信息，例如：是否能用匿名登录，是否有可写的FTP目录，是否能用Telnet，httpd是否用root在运行，等等。在获得目标主机TCP/IP端口和其对应的网络访问服务的相关信息后，与网络漏洞扫描系统提供的漏洞库进行匹配，如果满足匹配条件，则视为漏洞存在。此外，通过模拟黑客的进攻手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱势口令等，也是扫描模块的实现方法之一。如果模拟攻击成功，则视为漏洞存在。在匹配原理上，漏洞扫描系统主要采用的是基于规则的匹配技术，即根据安全专家对网络系统安全漏洞、黑客攻击案例的分析和系统管理员关于网络系统安全配置的实际经验，形成一套标准的系统漏洞库，然后在此基础之上构成相应的匹配规则，由程序自动进行系统漏洞扫描的分析工作。所谓基于规则是基于一套由专家经验事先定义的规则的匹配系统。例如，在对TCP 80端口的扫描中，如果发现/cgi-bin/phf或/cgi-bin/Count.cgi，根据专家经验以及CGI程序的共享性和标准化，可以推知该WWW服务存在两个CGI漏洞。同时应当说明的是，基于规则的匹配系统也有其局限性，因为作为这类系统的基础的推理规则一般都是根据已知的安全漏洞进行安排和策划的，而对网络系统的很多危险的威胁是来自未知的安全漏洞，这一点和PC杀毒很相似。实现一个基于规则的匹配系统本质上是一个知识工程问题，而且其智能应当能够随着经验的积累而增加，其自学习能力能够进行规则的扩充和修正，即是系统漏洞库的扩充和修正。当然这样的能力目前还需要在专家的指导和参与下才能实现。但是，也应该看到，受漏洞库覆盖范围的限制，部分系统漏洞也可能不会触发任何一个规则，从而不被检测到。

7.4.3 漏洞处理策略

漏洞形成的原因形形色色、不一而足，最常见的主要包含以下类型的漏洞：CGI脚本漏洞、POP3漏洞、FTP漏洞、SSH漏洞、HTTP漏洞、SMTP漏洞、IMAP漏洞、后门漏洞、RPC漏洞、DNS漏洞等。下面将以CGI脚本漏洞和SMTP漏洞为例来简单说明漏洞库的编制以及漏洞处理策略。

1. CGI脚本漏洞

CGI脚本是实现Web交互功能的重要手段。Shell脚本、Perl程序和C可执行程序是CGI

脚本最常采用的形式。由于程序编写上的疏忽，很多 CGI 脚本都存在漏洞，根据所收集的漏洞信息，CGI 漏洞的危害主要有 3 种：

（1）缓冲区溢出攻击。这种攻击实质是不遵守规则、歪曲或违反页面中建立的某个限制或约束。大部分 CGI 脚本是作为 HTML 表单的后台运行的，负责处理由用户输入的信息并提供某种定制的输出。因为在这种情况下，大部分 CGI 脚本编写时都等待某种特定格式的数据。然而，黑客可以有许多方法绕过这些预定义的格式而给脚本发送一些看起来是随机的数据。此时，由于 CGI 脚本可能在对输入数据的有效性的判定上存在不足，缺少全面的输入验证和净化，导致攻击者能够将特殊的字符和本地系统命令结合起来，作为参数输入，从而使得 Web 服务器执行该命令。例如：

! /cgi-bin/phf

漏洞描述：Apache httpd 服务器程序（1.0.3 版本）的 PHF 脚本由于输入验证中遗失了对换行符（"\n"，十六进制为 0x0a）的检查，从而可用于转义脚本，诱骗 Web 服务器程序的本地语法运行该转义符后的任何内容。

如果受攻击的 Web 服务器程序的执行用户具有/etc/passwd 文件的读权限，那么 URL 为 http://www.somedomain.org/cgi-bin/phf? Qalias=x%0a/bin/cat%20/etc/passwd 时将输出该文件的内容。

解决方案：自行修改该脚本，加入对"\n"的检验，或者暂停使用该脚本。

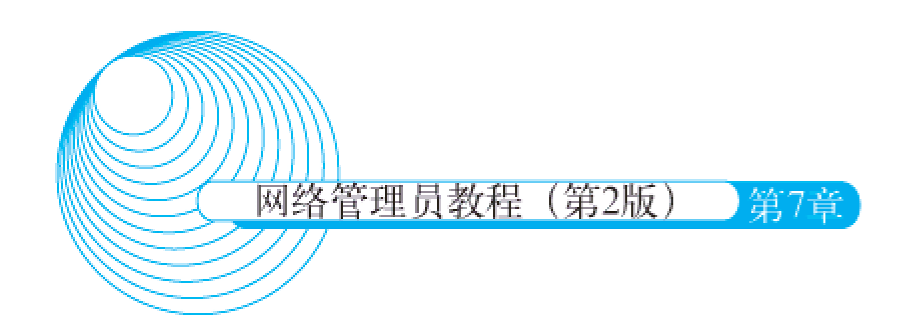
（2）数据验证型溢出攻击。由于 CGI 程序本身或程序调用的函数缺乏对用户输入数据的合法性检查，未能滤除一些特殊字符，使得入侵者可以通过构造请求来达到入侵的目的。比如，缺乏对"../"的过滤，可能导致入侵者读取系统的任意文件。例如：

!! /shop.cgi

漏洞描述：shop.cgi/shop.pl 支持 SSL，包含多种验证模块，配置文件是 shop.cfg。http://example.com/cgi-bin/shop.cgi/page=products.htm/SID=SHOPPING_ID_HERE 是正常的 URL 语法。于是带有客户信息的 products.htm 文件被显示出来。$page 变量的值是通过 open()调用打开的，open()调用本身并没有做任何输入/访问验证，也没有任何边界检查，诸如：http://example.com/cgi-bin/shop.cgi/page=../../../../etc/passw。这样的 URL 请求是合法的，于是/etc/passwd 就会被打开并显示出来。

解决方案：考虑利用正则表达式增加输入验证，过滤诸如../ 和 .\./. 之类的字符组合，也可以增加一个变量限制目录遍历深度。结合这两种技术，就可以限制来自潜在攻击者的任意目录遍历行为。

（3）信息泄漏。一些 CGI 程序所提供的功能自身违背安全性要求，如损害了信息的保密性，极易被入侵者利用。例如：



! /webpage. cgi

漏洞描述：当 URL 请求的文件不存在时，webpage. cgi 会向客户端浏览器返回某些敏感信息，比如脚本所在路径、HTTP 根目录所在路径、Perl 版本、server_admin、server_name、PATH 环境变量等。这就可以为进一步的攻击做准备。

解决方案：在浏览器中禁止 Java Applet。目前，大多数网站均使用免费的公共 CGI 脚本程序去驱动各自的 Web 服务，如此导致有缺陷的 CGI 脚本在因特网上泛滥开来。因此，对 CGI 脚本的安全性应高度重视。

2. SMTP 漏洞

SMTP(Simple Mail Transfer Protocol，简单邮件传输协议)是用来发送邮件的协议，其服务守护程序是 Sendmail。Sendmail 因为大而复杂，配置又十分麻烦，所以一度曾是 UNIX 上漏洞最多的程序，著名的蠕虫病毒就是利用 Sendmail 旧版本上的一个 DEBUG 命令的漏洞而从一个系统传播到另一个系统的。又如：利用 ETRN 命令可使 Sendmail 停止响应(即拒绝服务)。当 Sendmail 接收到 ETRN 命令时，它将调用 fork()。此时子进程将代替父进程发送响应输出，而父进程将不再响应 send()/write()错误。因此攻击者可发送大量 ETRN 命令，然后中断连接，这会使父进程连续地调用 fork()和 sleep(5)，而无法恢复正常的响应。

攻击者利用这个漏洞可以产生大量的“不可用”Sendmail 子进程，导致 Sendmail 长时间挂起(即使攻击者的网络带宽和资源很少)。直接的后果就是耗尽所有的服务器内存(Linux 2.0 内核将崩溃，出错信息为 no memory for Sendmail、no memory for klogd 或其他)。Sendmail 服务程序不断地升级，同时新的漏洞也不断地出现。一个不经意的错误，往往成了可怕的隐患。Sendmail 高级版本中仍存在着种种漏洞，仅举两例说明如下。

1) !! Sendmail 8.7～8.8.2

漏洞描述：Sendmail 版本 8.7～8.8.2 存在一个可获得超级用户权限的漏洞。Sendmail 服务一般作为守护进程运行，在标准 SMTP 端口(通常是 25 号端口)“监听”连接请求。超级用户是唯一允许以这种方式启动 Sendmail 服务的，因为 Sendmail 协议中有代码强制执行这种限制。但由于一个编码错误，任何本地用户都可能绕过检查，以守护进程的方式启动 Sendmail。通过改变 Sendmail 的邮件环境，用户可以超级用户的权限令 Sendmail 执行任意程序。

解决方案：升级到 Sendmail 8.10 以上的版本。

2) ! Sendmail~8.9.3

漏洞描述：mail. local 是 Sendmail 里面的一个程序，它被用作本地邮件的传送代理。mail. local 使用 LMTP(本地邮件传输协议)接受标准输入并发信给用户。当在 LMTP 模式下时，mail. local 处理的消息以“.\n”开始。因此，可以发送一个 2047 字节的、以“.\n”开头的字符串，那么这个字符串后面的内容就会被 mail. local 当做 LMTP 命令来处理。这样 sendmail 的日志

或者过滤机制就失去了作用。另一个问题是，当 LMTP 命令被执行的时候，mail. local 可能会产生结果输出。但是 sendmail 并不知道，所以不会去读 I/O buffer。这些结果输出如果很多，就会导致 sendmail 和 mail. local 死锁，I/O Buffer 也会被填满。

解决方案：sendmail 8.10 以上版本已经解决了 deadlock/LMTP 问题。

7.5 网络防病毒系统

7.5.1 计算机病毒简介

1. 计算机病毒的概念

“计算机病毒”是一段非常短的，通常只有几千个字节，会不断自我复制、隐藏和感染其他程序或计算机的程序代码。当执行时，它把自己传播到其他计算机系统、程序里。首先它把自己复制在一个没有被感染的程序或文档里，当这个程序或文档执行任何指令时，计算机病毒就会包括在指令里。根据计算机病毒编制者的动机，这些指令可以做任何事，并且导致不同的影响。其中包括显示一段信息、删除文档或有目的地改变数据。有些情况下，计算机病毒并没有破坏指令的企图，但取而代之就是占据磁盘空间、中央处理器时间或网络的连接。

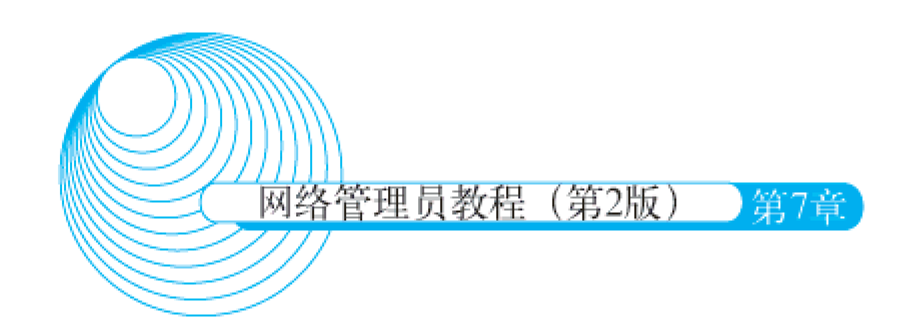
携带有计算机病毒的计算机程序被称为计算机病毒载体或被感染程序。计算机病毒的再生机制，即它的传染机制却是使计算机病毒代码强行传染到一切可传染的程序之上，迅速地在一台计算机内，甚至在一群计算机之间进行传染、扩散。每一台被感染了计算机病毒的计算机，本身既是一个受害者，又是一个新的计算机病毒传染源。

感染计算机病毒的计算机往往在一定程度上丧失或部分丧失了正常工作的能力，如运行速度降低、功能失常、文件和数据丢失，同时计算机病毒通过各种可能的渠道，如软盘、光盘、计算机网络去传染其他计算机。通过数据共享的途径，计算机病毒会非常迅速地蔓延开，若不加以控制，就会在短时间内传遍世界各个角落。可见计算机病毒防范的问题是一个全球性的问题。

随着因特网技术的发展，计算机病毒的定义正在逐步发生着变化，与计算机病毒的特征和危害有类似之处的“特洛伊木马”和“蠕虫”从广义的角度而言也可归为计算机病毒。下面是这两者的特点：

特洛伊木马是一种潜伏执行非授权功能的技术，它在正常程序中存放秘密指令，使计算机在仍能完成原先指定任务的情况下，执行非授权功能。特洛伊木马的关键是采用潜伏机制来执行非授权的功能。特洛伊木马通常又称为黑客程序。

“蠕虫”(Worm)是一个程序或程序序列，通过分布式网络来扩散传播特定的信息或错误，进而造成网络服务遭到拒绝并发生死锁或系统崩溃。蠕虫病毒的危害日益显著，“野蛮蠕虫病毒 ”(Wscript. Kak. Worm 或 Wscript. Kak. A)就是最近发生的影响极大的一例。



综合上述观点，在《中华人民共和国计算机信息系统安全保护条例》中，其中第二十八条中明确指出："计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。"此定义具有法律性、权威性。

2. 计算机病毒的特性

（1）传染性。计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，就与系统中的程序连接在一起，并不断地去传染（连接或覆盖）其他未被感染的程序。正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的。而计算机病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道，如磁盘、计算机网络去传染其他的计算机。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

（2）隐蔽性。计算机病毒通常附着在正常程序中或磁盘较隐蔽的地方，目的是不让用户发现它的存在。不经过程序代码分析或计算机病毒代码扫描，计算机病毒程序与正常程序是不容易区别开来的。在没有防护措施的情况下，计算机病毒程序经运行取得系统控制权后，可以在不到 1 秒钟的时间里传染几百个程序，而且在屏幕上没有任何异常显示，这种现象就是计算机病毒传染的隐蔽性。正是由于这隐蔽性，计算机病毒得以在用户没有察觉的情况下游荡于世界上百万台计算机中。计算机病毒的隐蔽性表现在两个方面：一是传染的隐蔽性，二是计算机病毒程序存在的隐蔽性。

（3）潜伏性。大部分的计算机病毒感染系统之后一般不会马上发作，它可长期隐藏在系统中，只有在满足其特定条件时才启动其表现（破坏）模块，在此期间，它就可以对系统和文件进行大肆传染。潜伏性愈好，其在系统中的存在时间就会愈久，计算机病毒的传染范围就会愈大。在潜伏期间计算机病毒程序不用专用检测程序是一般检查不出来的，因此计算机病毒静静地躲在磁盘或磁带里，除了传染外不做什么破坏，一旦条件满足就会发作。计算机病毒使用的触发条件主要有以下 3 种：

① 利用计算机内的时钟提供的时间作为触发器；

② 利用计算机病毒体内自带的计数器作为触发器；

③ 利用计算机内执行的某些特定操作作为触发器。

（4）破坏性。任何计算机病毒只要侵入系统，都会对系统及应用程序产生程度不同的影响。轻者会降低计算机工作效率，占用系统资源，重者可导致系统崩溃。这些都取决于计算机病毒编制者的意愿。几乎由软件手段能触及到计算机资源的地方均可能受到计算机病毒的破坏，例如有以下几个方面：攻击系统数据区，攻击部位包括引导扇区、FAT 表、文件目录；攻击文件；攻

击内存；干扰系统运行，如无法操作文件、重启动、死机等；导致系统性能下降；攻击磁盘，造成不能访问磁盘、无法写入等；扰乱屏幕显示；干扰键盘操作；喇叭发声；攻击 CMOS；干扰外设，如无法访问打印机等。

（5）针对性。计算机病毒都是针对某一种或几种计算机和特定的操作系统。例如，有针对 PC 及其兼容机的，有针对 Macintosh 的，有针对 UNIX 和 Linux 操作系统的，还有针对应用软件的，例如 Office 的宏病毒。

（6）衍生性。计算机病毒的衍生性是指计算机病毒编制者或者其他人将某个计算机病毒进行一定的修改后，使其衍生为一种与原先版本不同的计算机病毒，后者可能与原先的计算机病毒有很相似的特征，这时称其为原先计算机病毒的一个变种，如果衍生的计算机病毒已经与以前的计算机病毒有了很大甚至根本性的差别，此时就会将其认为是一种新的计算机病毒。新的计算机病毒可能比以前的计算机病毒具有更大的危害性。

（7）寄生性。计算机病毒的寄生性是指，一般的计算机病毒程序都是依附于某个宿主程序中，依赖于宿主程序而生存，并且通过宿主程序的执行而传播。蠕虫和特洛伊木马程序则是例外，它们并不是依附在某个程序或文件中，其本身就是完全包含有恶意的计算机代码，这也是二者与一般计算机病毒的区别。所以，计算机病毒防范软件发现此类程序后，通常的解决方法就是将其删除并修改相应的系统注册表。

（8）未知性。计算机病毒的未知性体现在两个方面：首先是计算机病毒的侵入、传播和发作是不可预见的，有时即使安装了实时计算机病毒防火墙，也会由于各种原因造成不能完全阻隔某些计算机病毒的侵入。其次，计算机病毒的发展速度远远超出了人们的想象，新的计算机病毒不断地涌现，但是如何出现以及如何防范却是永远不可预料的。

3. 计算机病毒的分类

目前，由于计算机网络及其现代通信技术的发展，从而使病毒的含义有所扩展，一般将病毒、网络蠕虫、黑客有害程序特洛伊木马等都称为病毒。

计算机病毒的分类方法有许多种，比如可以按照计算机病毒的破坏性质划分、根据计算机病毒所攻击的操作系统划分、根据计算机病毒的传播方式划分等，但是按照最通用的区分方式，即根据其感染的途径以及采用的技术区分，计算机病毒可分为文件型计算机病毒、引导型计算机病毒、宏病毒和目录（链接）型计算机病毒。

1）文件型计算机病毒

文件型计算机病毒感染可执行文件（包括 exe 文件和 com 文件）。一旦直接或间接地执行了这些受计算机病毒感染的程序，计算机病毒就会按照编制者的意图对系统进行破坏，这些计算机病毒还可细分为以下类别。

（1）驻留型计算机病毒：一旦此类计算机病毒被执行，它们会先检查当前系统是否满足事

先设定好的一系列条件(包括日期、时间等)。如果没有满足,它们就会在内存中“等候”其他程序的执行。此间,如果操作系统执行了某个操作,某个未感染计算机病毒的文件(或程序)被调用,计算机病毒就会将其感染,这一步骤是通过将其本身的恶意代码添加到源文件中实现的。

(2) 主动型计算机病毒:此类型计算机病毒被执行时,它们会主动地试图复制自己(即复制自身的代码)。一旦某种条件满足后,它们就会主动地去感染当前目录下以及在 autoexec. bat 文件(该文件总是位于根目录下,它负责在计算机引导时执行某些特定的动作)中指定的路径下的文件。对于这类计算机病毒,比较容易清除带毒文件中的恶意代码并将其还原到初始的正常状态。

(3) 覆盖型计算机病毒:顾名思义,此类计算机病毒的特征是计算机病毒将会覆盖其所感染文件中的数据,也就是说,一旦某个文件感染了此类计算机病毒,即使将带毒文件中的恶意代码清除掉,至少文件中被其覆盖的那部分内容永远不能恢复。某些覆盖型计算机病毒是常驻内存的。对于这类计算机病毒而言,尽管文件不能恢复,但还是可以清除其中的计算机病毒代码,这样做有可能恢复一部分数据。

(4) 伴随型计算机病毒:为了达到感染的目的,伴随型计算机病毒可以驻留在内存中等候某个程序执行(此时表现为驻留型计算机病毒)或者直接复制自己(此时表现为主动型计算机病毒)。与覆盖型计算机病毒和驻留型计算机病毒不同,伴随型计算机病毒不会修改其所感染的文件。当操作系统工作时,它将会调用某些程序,如果有两个同名但扩展名不同的文件(一个是 exe 文件,另一个为 com 文件),操作系统总是会先调用 com 文件。伴随型计算机病毒利用了操作系统的这一特性,如果有一个可执行的 exe 文件,计算机病毒将会创建另外一个文件名相同,但扩展名为 com 的文件,这样做可以迷惑用户。新的文件其实就是计算机病毒本身的代码。如果操作系统发现系统中有两个同名文件,将会先执行 com 文件,因此就会执行计算机病毒代码。一旦计算机病毒被执行,它将会将控制权交还给操作系统以便执行原先的 exe 文件。在这种方式下,用户不容易知道计算机病毒已经被激活。

2) 引导型计算机病毒

引导型计算机病毒影响软盘或硬盘的引导扇区。引导扇区是磁盘中至关重要的部分,其中包含了磁盘本身的信息以及用以引导计算机的一个程序。

引导型计算机病毒不会感染文件,也就是说如果某个软盘感染了引导型计算机病毒,但是只要不用它去引导计算机,其中的数据文件将不会受到影响。

如果用带有引导型计算机病毒的软盘引导计算机,它们就通过以下步骤感染系统:

(1) 它会首先在内存中保留一个位置以便其他程序不能占用该部分内存。

(2) 然后计算机病毒将自己复制到该保留区域。

(3) 此后计算机病毒会不断截取操作系统服务。每次当操作系统调用文件存取功能时,计算机病毒就会夺取系统控制权。它首先检查被存取文件是否已经被感染了计算机病毒,如果没

有感染，计算机病毒就会执行复制恶意代码的操作。

(4) 最后计算机病毒会将干净的引导扇区内容写回到其原先的位置，并将控制权交换给操作系统。在这种方式下，尽管计算机病毒还会继续发作，但用户觉察不到任何异样。

3) 宏病毒

前面提到的计算机病毒都是感染可执行文件(exe 文件或 com 文件)，而宏病毒与之不同，宏病毒感染的对象是使用某些程序创建的文本文档、数据库、电子表格等文件，这些类型的文件都能够在文件内部嵌入宏(macro)。它们不依赖于操作系统，但是可以使用户在文档中执行特定的操作。这些小程序的功能有点类似于批命令，能够执行一系列的操作，而看上去就像是只执行了一个命令一样，因此可以节省用户的时间。

宏作为一种程序，同样可以被感染，因此也成为计算机病毒的目标。当某个文档中的宏被打开后，它们会被自动加载并立即执行(或根据用户的需要以后执行)，计算机病毒就可以按照程序所设计的意图执行相应的动作。值得十分注意的是，宏病毒的传播速度极为迅速并能带来极大的危害。

4) 目录(链接)计算机病毒

操作系统总是会不断读取计算机中的这些文件信息，包括文件名及其存储位置信息。操作系统会赋予每个文件一个文件名和它的存储位置，然后，当用户每次使用该文件时就会调用这些信息。目录(链接)计算机病毒会修改文件存储位置信息以达到传染的目的。

操作系统运行程序时会立即寻找此程序的地址，然而，这类计算机病毒在操作系统寻找地址前获得地址信息，然后它会修改地址并指向计算机病毒的地址，并将正确的地址保存在其他地方。因此，当用户运行目标程序时，事实上是执行了计算机病毒程序。

此类计算机病毒能够修改硬盘上存储的所有文件的地址，因此能够感染所有这些文件。尽管目录(链接)计算机病毒不能感染网络驱动器或将其代码附加在受感染的文件中，但是它确实能够感染所有的硬盘驱动器。如果用户使用某些工具(如 SCANDISK 或 CHKDSK)检测受感染的磁盘，会发现大量的文件链接地址的错误，这些错误都是由此类计算机病毒造成的。发现这种情况后不要试图用上述软件去修复，否则情况会更糟。

7.5.2 网络病毒简介

具有开放性的因特网成为计算机病毒广泛传播的有利环境，而因特网本身的安全漏洞也为培育新一代病毒提供了良好的条件。人们为了让网页更加精彩漂亮、功能更加强大而开发出 ActiveX 技术和 Java 技术，然而病毒程序的制造者也利用这些技术，把病毒程序渗透到个人计算机中。这就是近两年兴起的第二代病毒，即所谓的“网络病毒”。

2000 年出现的“罗密欧与朱丽叶”病毒是一个非常典型的网络病毒，它改写了病毒的历史，该病毒与邮件病毒基本特性相同，它不再隐藏于电子邮件的附件中，而是直接存在于电子邮件

的正文中，一旦用户打开 Outlook 收发信件进行阅读，该病毒马上就发作，并将复制的新病毒通过邮件发送给别人，计算机用户无法躲避。

根据 ICSA（International Computer Security Association）实验室“2002 年度病毒传播趋势报告”的调查分析结果表明，目前病毒的传播方式主要是邮件传播和因特网传播，其中邮件传播比例高达 87％，因特网传播占 10％。其他传统的，经由磁盘、网络下载的病毒感染方式的传播率只有 3％，即 97％的病毒是通过网络传播的。

网络病毒的出现，似乎让病毒制造者的思路更加拓宽，近些年里，千奇百怪的网络病毒孕育而生。这些病毒具备更强的繁殖能力和破坏能力，他们不再局限于电子邮件中，而是直接进入 Web 服务器的网页代码中，当计算机用户浏览了带病毒的页面，系统就会被感染。当然这些病毒也不会放过自己寄生的服务器，在适当的时候，病毒会与服务器系统同归于尽。例如 2003 年的 8 月 12 日发作的“冲击波”病毒就让数万个企业的局域网瘫痪，企业的正常运作受到严重影响。现在以破坏正常的网络通信、偷窃数据为目的的病毒越来越多，它们和木马相配合，可以控制被感染的计算机，并将数据自动传给发送病毒者，造成涉密数据的泄漏，其危害程度极其严重。网络病毒相对于传统的计算机病毒，其特点及危害性主要表现在以下几个方面：

（1）破坏性强。网络病毒破坏性极强。直接影响网络工作，轻则降低速度，影响工作效率，重则使网络瘫痪。

（2）传播性强。网络病毒普遍具有较强的再生机制，一接触就可通过网络扩散与传染。一旦某个公用程序感染了病毒，那么病毒将很快在整个网络上传播，感染其他程序。

（3）具有潜伏性和可激发性。网络病毒与单机病毒一样，具有潜伏性和可激发性。在一定的环境下受到外界因素刺激，便能活跃起来，这就是病毒的激活。激活的本质是一种条件控制，此条件是多样化的，可以是内部时钟、系统日期和用户名称，也可以是在网络中进行的一次通信。一个病毒程序可以按照病毒设计者的预定要求，在某个服务器或客户机上激活，并向各网络用户发起攻击。

（4）针对性更强。网络病毒并非一定对网络上所有的计算机都进行感染与攻击，而是具有某种针对性。例如，有的网络病毒只能感染 IBM PC 工作地，有的却只能感染 Macintosh 计算机，有的病毒则专门感染使用 UNIX 操作系统的计算机。

（5）扩散面广。由于网络病毒能通过网络进行传播，所以其扩散面很大，一台 PC 机的病毒可以通过网络感染与之相连的众多机器。由网络病毒造成网络瘫痪的损失是难以估计的。一旦网络服务器被感染，其解毒所需的时间将是单机的几十倍以上。

（6）传播速度快。在单机环境下，病毒只能从一台计算机传播到另外一台计算机上，而在网络中则可以通过网络通信机制进行迅速扩散。

（7）难以彻底清除。单机上的计算机病毒有时可通过删除带毒文件、低级格式化硬盘等措施将病毒彻底清除。而在网络中，只要有一台工作站未能清除干净，就可能使整个网络重新被

病毒感染，甚至刚刚完成清除工作的一台工作站就有可能被网上另一台带毒工作站所感染。

鉴于网络病毒的以上特点，采用有效的网络病毒防治方法与技术就显得尤其重要了。目前，网络大都采用 C/S 模式，这就需要从服务器和客户机两个方面采取防治网络病毒的措施。

7.5.3 基于网络的防病毒系统

计算机病毒形式及传播途径日趋多样化，因此大型企业网络系统的防病毒工作已不再像单台计算机病毒的检测及清除那样简单，而且需要建立多层次的、立体的病毒防护体系，而且要具备完善的管理系统来设置和维护对病毒的防护策略。

1. 网络防病毒需求

建立了一个完整的网络平台之后，急需一个切实可行的防病毒解决方案，来确保整个网络的业务数据不受到病毒的破坏，日常工作不受病毒的侵扰。

1）网络的典型结构

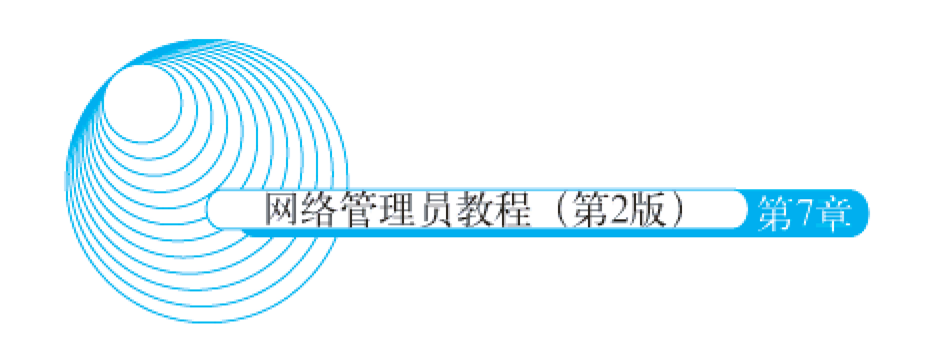
现代化企业计算机网络是在一定的硬件设备系统构架下对各种信息数据进行收集、处理加工和汇总的综合应用体系。目前大多数的企业网络都具有大致相似的体系结构，这种体系结构的相似性表现在网络的底层基本协议构架、操作系统、通信协议以及高层企业业务应用上，这就为通用的企业网络防病毒软件提供了某种程度的可以利用的共性。

从网络底层基本构架上，尽管不同的企业可能选择千差万别的联网设备，网络结构的复杂程度从简单的对等节点网络到三层交换复杂网络，但差不多全都是以太网结构，即基于 IEEE 802.2 和 IEEE 802.3 规范。事实已经证明，这是一种成熟、经济的桌面应用网络方案。目前应用最多的是一种交换到桌面的 10/100Mbps 快速以太网。

从网络的应用模式上看，现代企业网络都是基于一种叫做服务器/客户端的计算模式，即由服务器来处理关键性的业务逻辑和企业核心业务数据，客户端机器处理用户界面以及与用户的直接交互。服务器是网络的中枢和信息化核心，具有高性能、高可靠性、高可用性、I/O 吞吐能力强、存储容量大、联网和网络管理能力强等特点。客户端机器从硬件上没有特殊的要求，一般普通 PC 机就可以胜任。企业网络往往有一台或多台主要的业务服务器，在此之下分布着众多客户机或工作站，以及不同的应用服务器。根据不同的任务和功能服务，典型的服务器应用类型有：文件服务器、邮件服务器、Web 服务器、数据库服务器和应用服务器等。

从操作系统上看，企业网络的客户端基本上都是 Windows 平台，中小企业服务器一般采用 Windows NT/2000 系统，部分行业用户或大型企业的关键业务应用服务器采用 UNIX 操作系统。Windows 平台的特点是价格比较便宜，具有良好的图形用户界面；而 UNIX 系统的稳定性和大数据量可靠处理能力使得它更适合于关键性业务应用。

从通信协议上看，目前企业网络绝大部分采用 TCP/IP 协议。TCP/IP 本来是一种因特网



的通信协议，但是主流操作系统和绝大部分应用软件的支持以及它本身的发展，已经使得它足以承担从企业内部网到因特网的主要通信协议重任。当然，为了管理的方便或某些特殊的需求，在企业内部网上常见的协议也包括 NetBIOS、IPX/SPX 等。

2）网络的典型应用

当前，企业网络主要应用于文件和打印服务共享、办公自动化系统、企业业务（MIS）系统、因特网应用等领域。

（1）文件和打印共享：是企业建网的最初目的，也是计算机网络的最基本应用。有了网络，文件再也不用通过软盘拷来拷去，同时大文件的交换、应用程序共享等也变得更加方便，工作组的全体成员可以在自己的计算机上使用共享的打印机。

（2）办公自动化（OA）应用：企业网络应用达到了一定的层次，就需要一种更加方便的内部通信和消息传送机制，以及工作流程在计算机上的体现和基于网络的协同工作机制，对办公信息也更加要求规范化和一致化，而且能够将所有的办公文档汇集在一起，方便地进行统计和查找，按照不同的权限设置在企业成员之间共享。基于这些需求建立起来的应用系统，就是企业的办公自动化（OA）应用。目前的 OA 应用系统大都建立在一种叫做群件的软件平台上，最流行的群件软件有 Lotus 公司的 Domino/Notes 系统以及 Microsoft 的 Exchange/OutLook 系统。

（3）企业管理信息系统（MIS）：企业信息管理系统是能对企业管理的各种信息进行收集、分析、储存、传输、维护，为企业管理提供决策信息，是一个利用现代计算机信息及网络技术进行企业综合管理的系统工程。MIS 与 OA 的区别在于：MIS 系统管理的是高度结构化，数据粒度比较小的业务信息，比如财务数据，它的长项在于数据实时的统计查询和灵活的报表生成；而 OA 管理的是非结构化的数据，包括大规模的文本、图像、声音等，它的长项在于规范工作成员之间的工作流程和促进交流与协作。

企业应用 MIS 和 OA 系统进行业务数据管理和工作流程管理，这些系统都充分地利用了网络的数据交换特征，大量的文档、结构化或非结构化的业务数据通过网络来传输和处理。这种频繁和大规模的文件、数据交换也为病毒通过网络传播大开了便利之门。

（4）企业因特网应用：企业需要收发电子邮件，浏览外部网页，发布企业信息。所有这些都需要企业内部网与因特网之间连接畅通无阻。畅通的因特网连接使得企业方便地获取和发布信息的同时，也为病毒的乘虚而入创造了条件。

总之，企业应用需要网络的便利信息交换特性，病毒也可以充分利用网络的特性来达到它的传播目的。企业在充分地利用网络进行业务处理时，就不得不考虑网络的病毒防范问题，以保证关系企业命运的业务数据完整而不被破坏。

3）病毒在网络中的传播过程

目前，因特网已经成为病毒传播最大的来源，电子邮件和网络信息传递为病毒传播打开了高速的通道。企业网络化的发展也使病毒的传播速度大大提高，感染的范围也越来越广。可以

说，网络化带来了病毒传染的高效率，而病毒传染的高效率也对防病毒产品提出了新的要求。

近年来，全球的企业网络经历了网络病毒的不断侵袭。“爱虫”、“探险者”（Explore）、Matrix和冲击波病毒可以算是大名鼎鼎了。这些病毒几乎一夜之间让世界为之震惊，唤醒了人们对于网络防毒的重视。以 Remote Explore、Matri、LOVELETTER 和冲击波 4 个典型病毒为例，来说明网络病毒如何通过因特网进入企业网络并在内部快速传播。

（1）病毒 Remote Explore 算是网络病毒的“先驱者”，它于 1998 年爆发，至今仍是病毒发展历史中的一个重要标志。

Remote Explore 病毒通过盗取 Windows NT 域管理员的账号进行传播。如果一个具有管理员身份的用户执行了染毒的程序，该病毒便以服务（Service）的方式驻留内存，取名为 Remote Explore，并在染毒系统中安装文件\winnt\system32\drivers\ie403r. sys。这时，另一台 Windows NT 机器只要用同一管理员账号登录到染毒的机器中，该病毒就可以感染 Windows NT 局域网附加网络驱动器中的文件。当病毒被激活后，它便在共享的网络驱动器上随机选择一个文件夹，感染除. dll 或. tmp 扩展名以外的所有其他文件，连一些 DOS 下的 EXE 文件也同样难逃厄运。

（2）病毒 Matrix（还有许多别名）在 2000 年 8 月发源于德国，在当时它是一个危险级数相当高的病毒。该病毒之所以能够在全球范围内广泛且快速传播，是由于它具有网络蠕虫的特性，即利用因特网和局域网进行传播。

该病毒以邮件附件的形式传播。当接收者打开附件，该病毒便在网络系统内安装文件到 c:\windows 目录下，然后将系统内的 WSOCK32. DLL 删除，把 WSOCK32. MTX 更名为 WSOCK32. DLL。这样，受感染系统在发送邮件时增加自动发送附件的功能，附件即为蠕虫的副本。此外，病毒还能对网上邻居中的所有可用资源（映像驱动器）进行搜索，以便能够同本机进行文件传输，从而达到感染网络中其他机器的目的。

病毒通过创建 wininit. ini 文件，在每次系统启动后自动运行。另外，被安装的文件 MTX_. EXE还能够将系统连接到指定的站点，并下载新的病毒插件，以完成自我更新。

（3）病毒 LOVELETTER 于 2000 年 5 月发源于菲律宾。“爱虫”病毒可谓家喻户晓，它在全世界制造的恐慌给人们留下了深刻的教训。据统计，爱虫病毒在全球危及计算机 4500 万台，造成经济损失 100 亿美元。

“爱虫”病毒最大的特点是通过 E-mail 和 IRC 快速传播。在通过电子邮件传播时，它不放过地址簿中的每一个地址，而且，邮件的主题还是具有诱惑性的 I LOVE YOU。附件为 LOVE-LETTER-FOR-YOU. TXT. VBS，一旦用户打开附件，病毒便进行感染：搜索 Outlook 地址簿、IRC 连接、发送带有病毒的邮件、通过 IRC 感染其他用户。本机系统被感染后，爱虫病毒开始查找所有相连接的固定和移动的驱动器，用自身代码覆盖扩展名为 vbs、vbe、js、jse、css、wsh、sct 和 hta 的所有文件。而对于 jpg、jpeg 文件，爱虫病毒不仅用病毒代码覆盖原文件，还添加. vbs 扩展

名……

(4) Wrom. MSBlast. 6176(中文名为冲击波)，2003 年 8 月 12 日爆发，在短短一周之内，“冲击波”病毒至少攻击了全球 80％的 Windows 用户，使他们的计算机无法工作并反复重启，大量企业用户也未能幸免。该病毒还引发了 DoS 攻击，使多个国家的因特网也受到相当影响。

该病毒类型为蠕虫，利用 Windows 的 RPC 漏洞进行快速传播。病毒程序使用 UPX 压缩，仅有 6KB。该病毒具有如下行为：病毒添加注册表键值″windows auto update″＝″msblast. exe″在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下，以使蠕虫可以开机自动运行；攻击 RPC 服务默认端口，为传播自己做准备；监听 UDP 69 端口，当有服务请求，就发送 Msblast. exe 文件，然后发送命令到远端计算机(被攻击计算机)，以使其连接被感染计算机(本地计算机)下载并运行该病毒；如果当前月份大于 8 月，或当前日期大于 15 号，就对 Windowsupdate. com 实施 DoS 攻击。

从上面典型病毒传播方式可以看出，现代病毒在企业网络内部之所以能够快速而广泛传播，是因为它们充分利用了网络的特点。

一般来说，计算机网络的基本构成为网络服务器和网络节点站(包括有盘工作站，无盘工作站和远程工作站)。计算机病毒一般首先通过有盘工作站传播到软盘和硬盘，然后进入网络，进一步在网上传播。具体来说，其传播方式有如下几种：

- 病毒直接从有盘站复制到服务器中；
- 病毒先传染工作站，在工作站内存驻留，等运行网络盘内程序时再传染给服务器；
- 病毒先传染工作站，在工作站内存驻留，在运行时直接通过映像路径传染到服务器；
- 如果远程工作站被病毒侵入，病毒也可以通过通信中数据交换进入网络服务器中。

2. 网络病毒防护策略

基于网络系统的病毒防护体系主要包括以下几个方面的策略：

(1) 防毒一定要实现全方位、多层次防毒。一定要部署多层次病毒防线，如网关防毒、群件服务器、应用服务器防毒和客户端防毒，保证斩断病毒可以传播、寄生的每一个节点，实现病毒的全面防范。

(2) 网关防毒是整体防毒的首要防线。将网关防毒作为最重要的一道防线来部署，全面消除外来病毒的威胁，使得病毒不能再从网络传播进来，对内部网资源和系统资源造成消耗。同时，网关防毒这道防线上还要具备内容过滤功能，全面防范垃圾邮件的侵扰以及内部机密数据的外泄，在整个防毒系统中起到事半功倍的效果。

(3) 没有管理的防毒系统是无效的防毒系统。因此一定要保证整个防毒产品可以从管理系统中及时得到更新，同时又使得管理人员可以在任何时间、任何地点通过浏览器对整个防毒系统进行管理，使整个系统中任何一个节点都可以被管理人员随时管理，保证整个防毒系统有效、

及时地拦截病毒。

（4）服务是整体防毒系统中极为重要的一环。防病毒系统建立起来之后，能不能对病毒进行有效的防范，与病毒厂商能否提供及时、全面的服务有着极为重要的关系。这一方面要求厂商要以全球化的防毒体系为基础，另一方面也要求厂商能有足够的本地化技术人员作依托，不管是对系统使用中出现的问题，还是用户发现的可疑文件，都能进行快速的分析和提供可行的解决方案。

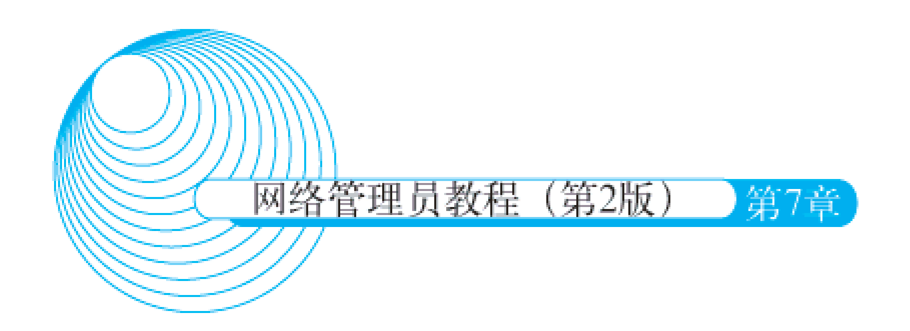
3. 网络防病毒系统组织形式

（1）系统中心统一管理。网络病毒防护系统结构为了提高杀毒的效率和稳定性，通常可采用多系统中心的构架，分层次管理，系统可构建一个一级系统中心，作为整个网络防病毒系统总管理中心；在各部门安装二级系统中心，各个二级系统中心负责管理本单位的机器，同时接受一级系统中心的命令和管理，向一级系统中心汇报本中心情况。所有的二级系统中心都由一级系统中心统一管理。网络病毒防护系统可通过系统中心管理所有已经安装了客户端和服务器端的局域网内的主机，包括在Windows 9x、Windows 2000 Professional、Windows 2000 Server、Windows NT/XP、UNIX、Linux等操作系统上的防病毒软件。也就是说，通过系统中心可以控制网络内所有的机器统一杀毒，在同一时间杀除所有病毒，从而解决网络环境下机器的重复感染问题。

（2）远程安装升级。因为网络用户层次的多样性，在实施网络病毒防护系统时一定要考虑到用户对网络安全的认识水平，通常需提供远程安装和自动升级等功能，在系统中心就可以给客户端安装杀毒软件的客户端，在系统中心病毒库升级后，客户端自动从系统中心升级。整个杀毒工作由网管人员统一完成，可以不用用户进行人工干预，这就减少了对用户管理的依赖。

（3）一般客户端的防毒。客户端的杀毒软件既可以由系统中心安装，也可以在本机安装，安装运行后即可被系统中心识别，系统中心可以控制本机和客户端软件的设置和杀毒，而客户端的机器也可以自己杀毒并将杀毒情况传给系统中心，以便网管人员及时了解局域网内的病毒发作情况；服务器端的防毒，服务器端的杀毒原理和客户端类似，只是将客户端软件换成了专门为服务器系统设计的服务器端软件。

（4）防病毒过滤网关。单机版防病毒软件难以做到及时、统一更新病毒代码库；网络版防病毒软件固有的缺陷是，携带病毒的邮件已经到达客户机之后才得到发现和处理，而且部署成本比较高。为此，与单机版、网络版防病毒系统之间“相互补充”的防毒过滤网关应运而生，防毒过滤网关实际上就是企业级病毒防火墙，可谓“一夫当关、万夫莫开”。通常防病毒过滤网关通过部署在用户内部网与外部网的接入点，实现邮件病毒过滤及因特网病毒过滤，可以简单、高效地对用户网络来自因特网的病毒威胁实现强有力的深层病毒防护。该类产品由邮件病毒过滤、网页病毒过滤和FTP下载过滤等几大防毒功能模块构成，其中最重要的是邮件病毒过滤功能。



（5）硬件防病毒网关。硬件防毒网关类产品相比其客户端、服务器软件类防毒产品有以下几个特色：

① 高效稳定。由于采用独立的硬件平台，大大提高了系统的稳定性和查杀病毒的效率。

② 操作简单、管理方便。硬件防毒网关类产品一般采用 B/S 管理构架，友好的图形管理界面可供用户方便地对设备进行简便易行的配置。

③ 接入方式简单易行。

④ 免维护。可远程自动更新代码和系统升级，无需管理员日常维护。

⑤ 容错与集群，系统通过集群模块，在容错的同时，线性地增加处理能力，满足高带宽的网关杀毒需要。

7.5.4 网络防病毒系统安装、配置实例

目前，国内有部分厂家研制出自己的网络版防病毒、安全网关系统，如方正信息安全公司的方正熊猫网络版防病毒系统、安全网关系统等，国外的如 Symantec 等防病毒厂商。下面仅以方正熊猫网络版为例对网络版防病毒的安装和配置加以说明。

1. 用户网络环境的简单描述

在用户的网络里面有 1000 个用户，通过地址转换的方式访问因特网，用户的操作系统主要是 Windows 平台，同时对外提供邮件、Web、FTP 等相关服务。目前用户的网络里面已经有防火墙、入侵检测等相关产品，但是没有任何防病毒措施。为了便于集中管理和日志查看，通常在用户的网络里面部署网络版防病毒系统和安全网关系统，它们的作用如下所述。

- 安全网关系统：高速的互联网技术发展，让很多黑客程序、病毒程序以及针对操作系统漏洞的攻击现象频繁发生，最终让用户的网络处于一种瘫痪状态。因此在出口部署方正熊猫安全网关系统，目标是在网络边界或 Internet 网关处提供全面的病毒防护，而该病毒防护设备是即插即用的，不需要改变任何 Internet 设置，并对所有应用及服务透明。由于内部用户并发连接比较多，为了防止网络访问性能的下降，因此在出口部署两台安全网关做负载均衡，分滩流量。
- 网络防病毒：在网络内所有的机器上部署网络版防病毒软件，防止用户共享文件、使用不同的介质等多种途径而感染病毒，同时配合安全网关系统帮助用户形成立体的病毒防护。拓扑如图 7-14 所示。

2. 网络版防病毒软件的构成

方正熊猫网络版防病毒软件 AdminSecure 由 AdminSecure 管理服务器、AdminSecure 控制台、AdminSecure 仓储服务器、AdminSecure 事件存储数据库、AdminSecure 通信代理 5 个组件

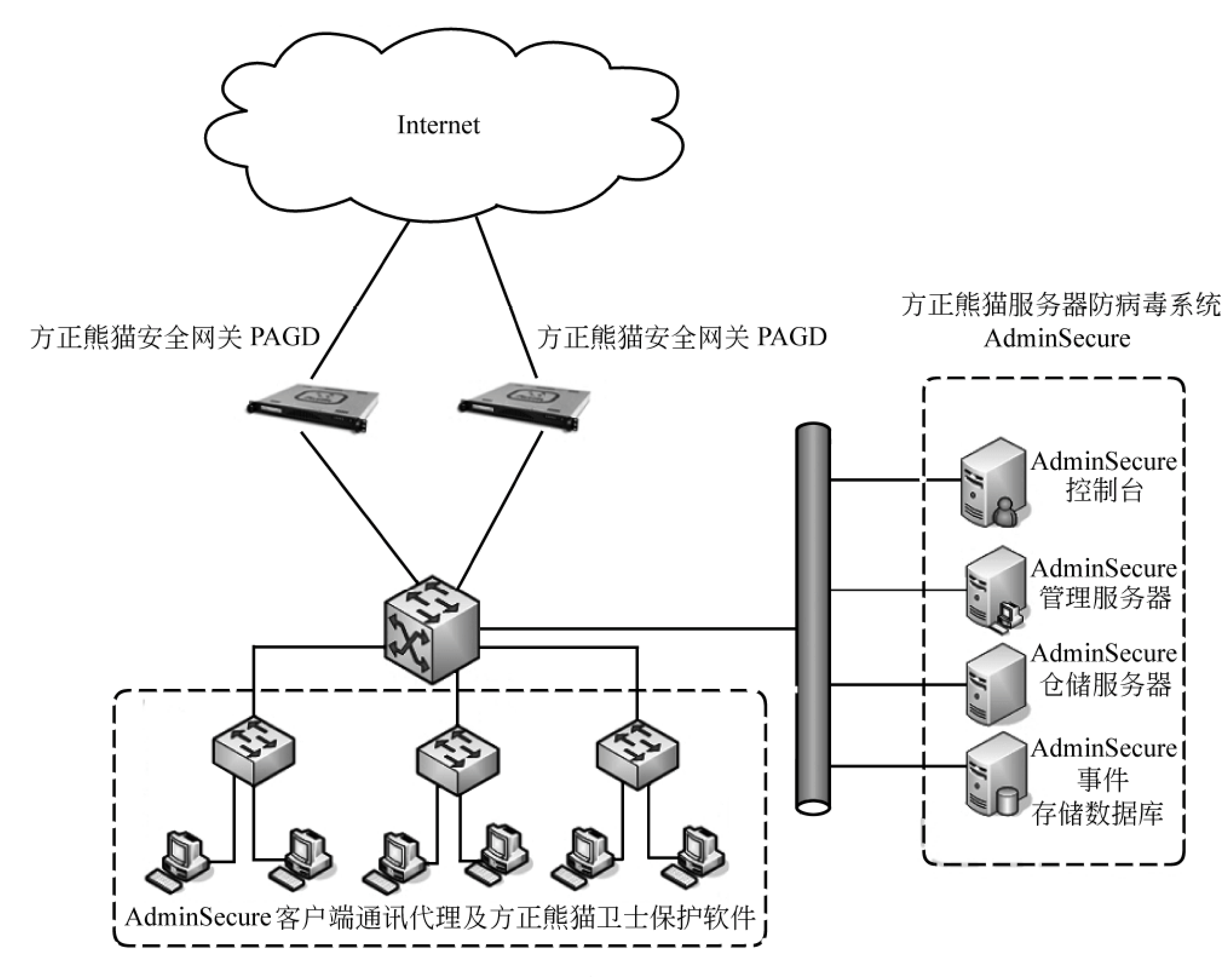


图 7-14　整体防病毒系统部署

构成。

以下分别描述这些组件的功能和特点：

(1) AdminSecure 管理服务器

- AdminSecure 的基础和核心
- 一个网络中通常只有一台管理服务器
- 以后台任务的方式执行管理员的指令
- 更新事件存储数据库中的管理信息数据
- 只能够安装在基于 NT 的计算机中

(2) AdminSecure 控制台

- 提供用户界面
- 用于执行管理任务
- 控制组织树
- 可安装在任何 Windows 计算机上

- 网络中可有多个控制台

(3) AdminSecure 仓储服务器

- 存储所有的防病毒软件的文件，包括病毒特征码库文件
- 负责更新所有的防病毒软件和病毒特征码库
- 一个网络中可安装多个仓储服务器
  - ◆ 主仓储服务器：从 Internet 更新
  - ◆ 备份仓储服务器：从主仓储服务器同步
- 每台仓储服务器最多为 2000 台计算机提供分发

(4) AdminSecure 事件存储数据库

- 存储所有管理信息数据供管理服务器使用
- 可使用 AdminSecure 内置的数据库或网络中现有的数据库
- 可与 AdminSecure 协同工作
- MSDE 2000
- MS SQL Server 7 或以上版本

(5) AdminSecure 通信代理

- 负责各个计算机之间的网络通信
- 采用 XML 消息传递管理数据
- 必须安装在所有计算机上
- 在驻留的计算机上执行的任务
  - ◆ 收集被管理计算机的软硬件信息和病毒事件报告
  - ◆ 根据管理服务器的指示安装、配置和更新被管理计算机的防病毒软件
  - ◆ 根据管理服务器的指示在被管理计算机上启动病毒扫描
- 通信代理的分发方式
  - ◆ 从控制台直推
  - ◆ 通过网络登录脚本
  - ◆ 用独立安装包手工安装

3. AdminSecure 服务器安装

(1) 执行安装文件，选择语言版本，如图 7-15 所示。

(2) 单击“下一步”继续，如图 7-16 所示。

(3) 查看许可协议，选中接受该协议，如图 7-17 所示。

(4) 输入用户信息产品并激活产品，如图 7-18 所示。

(5) 选择安装类型，如果是初次安装，请选择“安装 Panda AdminSecure”，如图 7-19 所示。



图 7-15　选择语言版本

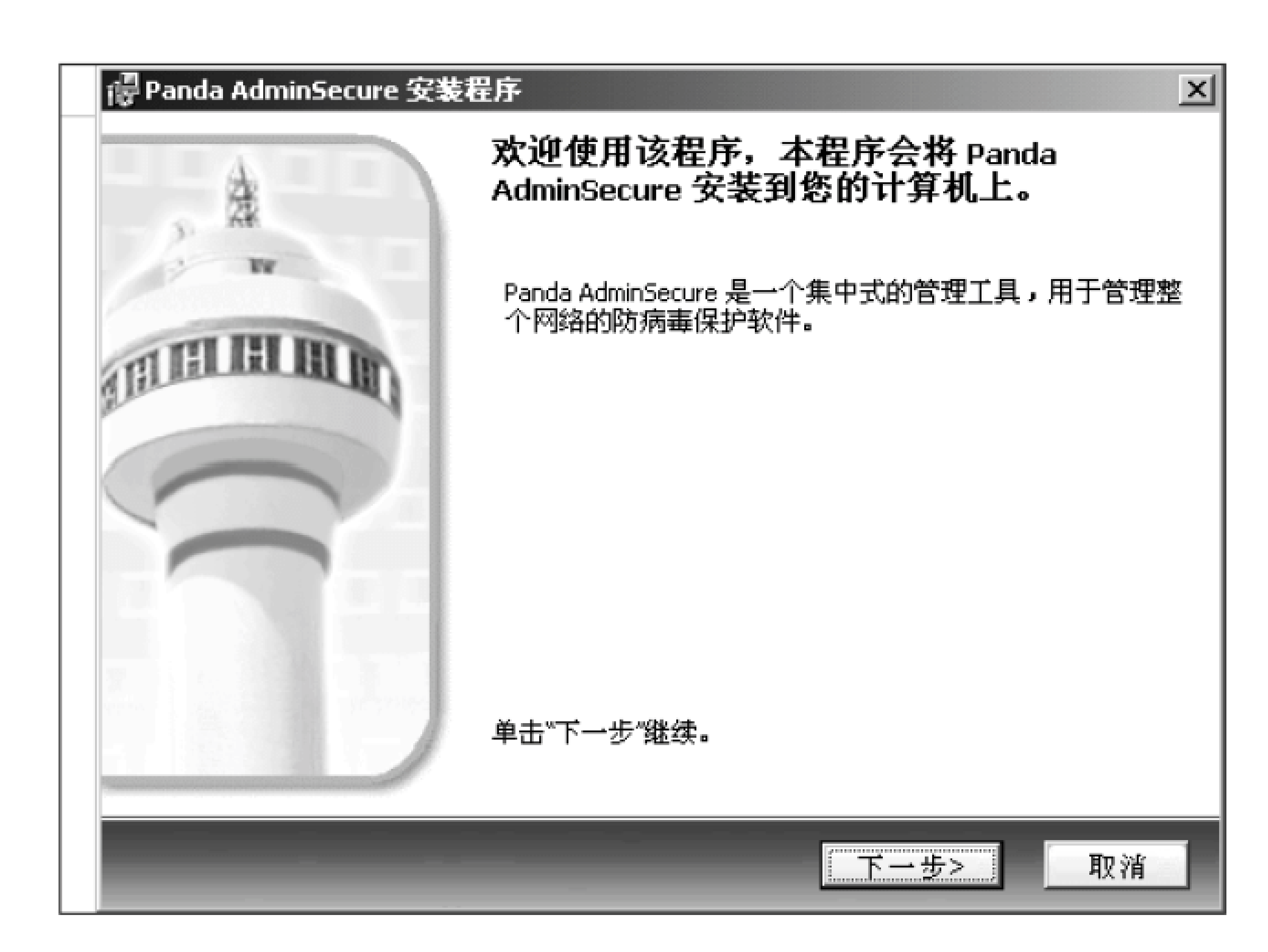


图 7-16　下一步安装

（6）在如图 7-20 所示对话框中，选择“是”继续安装。

（7）如果使用自带的 MSDE 数据库请选择“简单安装”，若是 SQL 数据库请选择“自定义安装”，如图 7-21 所示。

（8）选中“自动更新”让服务器定期更新病毒库，如图 7-22 所示。

（9）在图 7-23 所示对话框中，选择程序安装目录。

（10）确认无误后，选择“下一步”进行安装，打开如图 7-24 所示对话框。

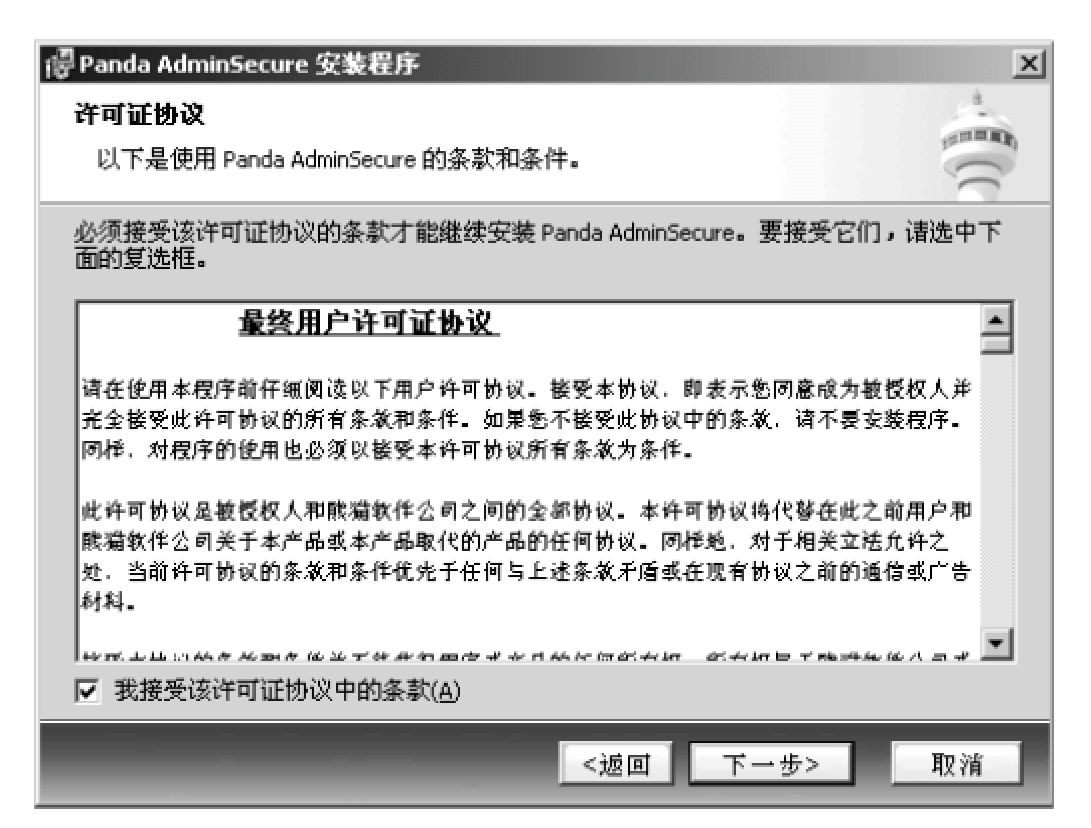


图 7-17　接受许可协议

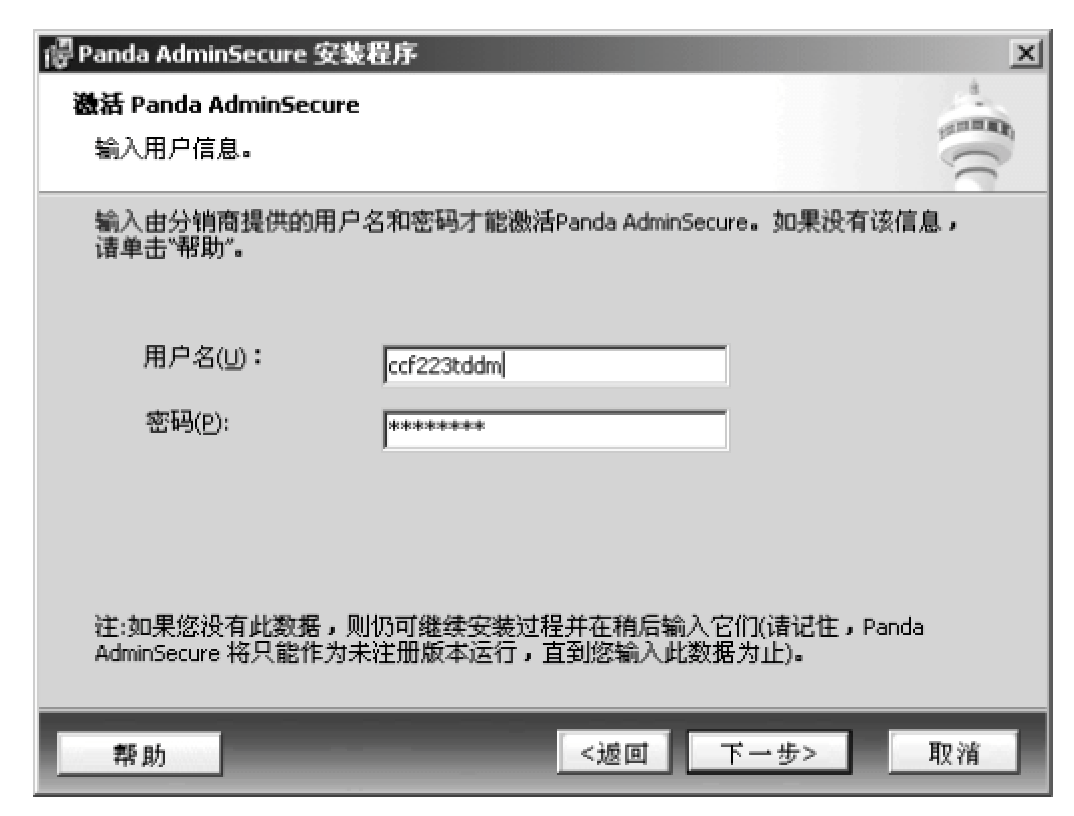


图 7-18　激活产品



图 7-19　选择安装类型



图 7-20　继续安装



图 7-21　选择自定义安装



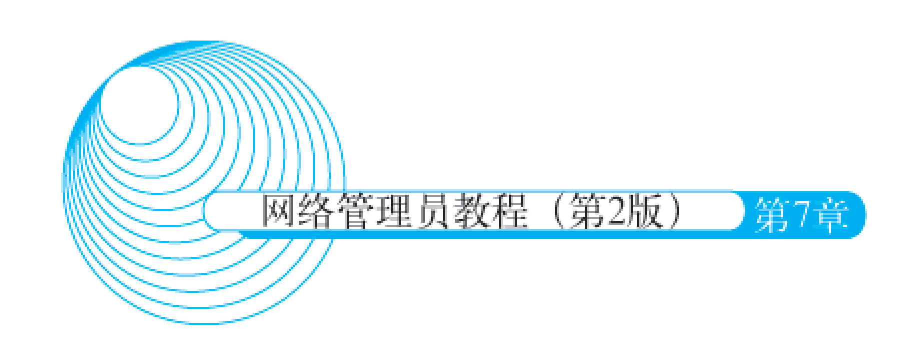
图 7-22　启用自动更新



图 7-23　选择程序安装目录



图 7-24　进行安装



（11）安装完成后，将在本机安装 AdminSecure 通信代理，在图 7-25 所示对话框中，单击“完成”安装成功。



图 7-25　完成安装

7.6　其他网络安全措施

7.6.1　物理安全

保证计算机系统各种设备的物理安全是整个计算机系统安全的前提，物理安全是保护计算机、网络设备、设施等免遭地震、水灾、火灾等事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。它主要体现在机房环境要求、设备物理防范和介质安全 3 个方面。

1. 环境安全

随着计算机硬件制造技术的飞速发展，计算机软、硬件性能已变得越来越稳定可靠了，计算机对环境的要求越来越低，现在放置普通微机的房间已不需要进行专门装修布置了，但有一些基本要求还是要达到的，例如放置计算机设备的房间要保持整洁，温、湿度适宜，应将计算机设备放置在通风良好的位置等。对系统所在环境的安全保护，如区域保护和灾难保护参见国家标准 GB50173－93《电子计算机机房设计规范》、GB2887－89《计算站场地技术条件》和 GB9361－88《计算站场地安全要求》。

2. 设备安全

设备安全主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及

电源保护等。电源系统要安插牢固，接触可靠，有过载保护功能，有独立电源开关，带有良好接地的三相插板，是经国家技术监督局检测的合格产品。对于存放重要数据的计算机，要加装后备式UPS电源，对于网管中心的服务器和网络关键节点设备，要加装在线式长延时UPS电源。

3. 媒介安全

包括媒介数据的安全及媒介本身的安全。对于存放重要数据的计算机设备，要有定期数据备份计划，用磁盘、光盘等介质及时备份数据，妥善存档保管。有数据恢复方案，在系统瘫痪或出现严重故障时，能够进行数据恢复。

4. 防火安全

为防止因火灾而导致的数据丢失，要有专用的计算机灭火设备。通常计算机火灾不适合使用干粉或泡沫灭火器，应使用1211系列灭火器。1211系列灭火器电绝缘性好，灭火后不留痕迹，适用于扑灭微机、精密仪器及小型带电设备等的初起灭火。另外，要定期检查灭火器压力表，通常1211灭火器压力在室温20℃时，应不低于1.0MPa。

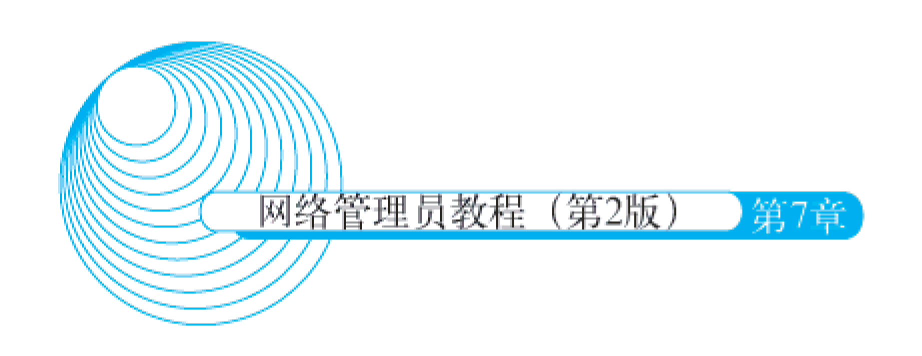
5. 保密安全

计算机系统的保密主要是指存放于磁盘上的文件、数据库等数据传输和存储的保密措施，应用于这方面的技术主要有访问控制、数据加密等。加密系统有数据加/解密卡、数据加密机、数据采编加密系统、抗辐射干扰器、电子印章系统等。涉密计算机信息系统保密设施的建设和实施是一个十分复杂的问题，是有严格的技术规范和操作规程的。涉密计算机网络必须遵守下述国家法律制度：

（1）对于计算机信息系统的建设和应用、安全保护等级、国际联网备案、计算机信息媒体进出境申报、计算机病毒及其有害数据的专管和计算机信息系统安全专用产品销售许可证等问题，国务院（国发[1994]147号）发布了《中华人民共和国计算机信息系统安全保护条例》，公安部还制订了强制性国家标准《计算机信息安全保护等级划分准则》，该准则于1999年9月13日经国家质量技术监督局发布，并于2001年1月1日起实施。

（2）对于信息安全保密，中共中央保密委员会办公室和国家保密局1998年6号联合发布了《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》。

（3）对于接入国际互联网应遵循的法律制度和规范，有国务院1996年第195号发布的《中华人民共和国计算机信息网络国际联网管理暂行规定》和国信办1997年发布的《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》、公安部1997年发布的《计算机信息网络国际联网安全保护管理办法》等。



7.6.2 电磁泄密及防护

1. 泄密渠道

为保证信息网络系统的物理安全，除对网络规划和场地、环境等要求之外，还要防止系统信息在空间的扩散。计算机系统通过电磁辐射使信息被截获而失秘的案例已经很多，在理论和技术支持下的验证工作也证实：这种截取距离在几百甚至可达千米的复原显示给计算机系统信息的保密工作带来了极大的危害。为了防止系统中的信息在空间上的扩散，通常是在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。这对重要的政策、军队、金融机构在兴建信息中心时都将成为首要设置的条件。

计算机主机及其附属电子设备如视频显示终端、打印机等在工作时不可避免地会产生电磁波辐射，这些辐射中携带有计算机正在进行处理的数据信息。尤其是显示器，由于显示的信息是给人阅读的，是不加任何保密措施的，所以其产生的辐射是最容易造成泄密的。使用专门的接收设备将这些电磁辐射接收下来，经过处理，就可恢复还原出原始信息。国外计算机应用比较早，对计算机设备的辐射问题早已有所研究，在1967年的计算机年会上美国科学家韦尔博士发表了阐述计算机系统脆弱性的论文，总结了计算机4个方面的脆弱性，即：处理器的辐射；通信线路的辐射；转换设备的辐射；输出设备的辐射。这是最早发表的研究计算机辐射安全的论文，但当时没有引起人们的注意。1983年，瑞典的一位科学家发表了一本名叫《泄密的计算机》的小册子，其中再次提到计算机的辐射泄漏问题。1985年，荷兰学者艾克在第三届计算机通信安全防护大会上，公开发表了他的有关计算机视频显示单元电磁辐射的研究报告，同时在现场用一台黑白电视机接收计算机辐射泄漏信号。他的报告在国际上引起强烈反响，从此人们开始认真对待这个问题。据有关报道，国外已研制出能在一千米之外接收还原计算机电磁辐射信息的设备，这种信息泄露的途径使敌对者能及时、准确、广泛、连续而且隐蔽地获取情报。计算机电磁辐射泄密问题已经引起了世界各个国家的高度重视，要防止这些信息在空中传播，必须采取防护和抑制电磁辐射泄密的专门技术措施，这方面的技术措施主要有：干扰技术、屏蔽技术和Tempest技术。

2. 防护手段

1）配置视频信息保护机（干扰器）

视频保护（干扰）技术又可分为白噪声干扰技术和相关干扰技术两种。白噪声干扰技术的原理是使用白噪声干扰器发出强于计算机电磁辐射信号的白噪声，将电磁辐射信号掩盖，起到阻碍和干扰接收的作用。这种方法有一定的作用，但由于要靠掩盖方式进行干扰，所以发射的功率必须足够强，而太强的白噪声功率会造成空间的电磁波污染；另外白噪声干扰也容易被接

收方使用较为简单的方法进行滤除或抑制解调接收。因此白噪声干扰技术在使用上有一定的局限性和弱点。

相关干扰技术较之白噪声干扰技术是一种更为有效和可行的干扰技术。相关干扰技术的原理是使用相关干扰器发出能自动跟踪计算机电磁辐射信号的相关干扰信号，使电磁辐射信号被扰乱，起到数据加密的效果，使接收方即使接收到电磁辐射信号也无法解调出信号所携带的真实信息。由于相关干扰不需靠掩盖电磁辐射信号来进行干扰，因此其发射功率无须很强，所以对环境的电磁污染也很小。相关干扰器使用简单，体积小巧，价格适宜，效果显著，最适合应用在单独工作的个人计算机上。我国现在已能生产出这种相关干扰器。

2）建造电磁屏蔽室

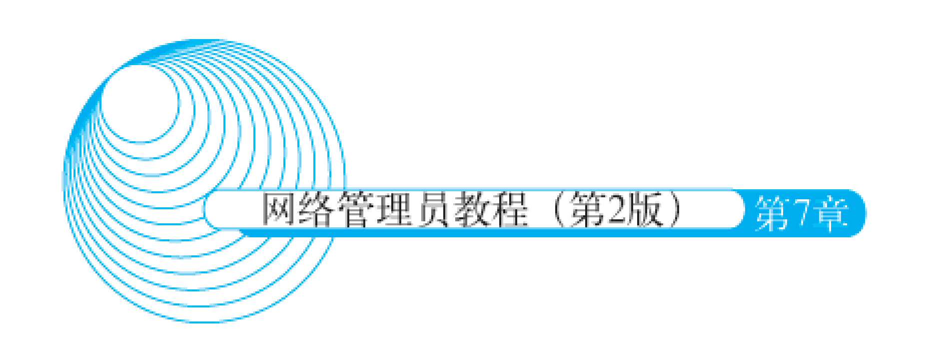
屏蔽技术的原理是使用导电性能良好的金属网或金属板造成6个面的屏蔽室或屏蔽笼，将产生电磁辐射的计算机设备包围起来并且良好接地，抑制和阻挡电磁波在空中传播。设计和安装良好的屏蔽室对电磁辐射的屏蔽效果比较好，能达到60～90dB以上。如美国研制的高性能的屏蔽室，其屏蔽效果对电场可达140dB，对微波场可达120dB，对磁场可达100dB。妨碍屏蔽技术普遍应用的问题是屏蔽室的设计安装施工要求相当高，造价非常昂贵，一般二三十平方米场地的屏蔽室的造价即需几十至上百万元。因此屏蔽技术较为适用于一些保密等级要求较高、较重要的大型计算机设备或多台小型计算机集中放置的场合，如国防军事计算中心、大型的军事指挥所、情报机构的计算中心等。

3）配置低辐射设备

Tempest技术即低辐射技术。这种技术是在设计和生产计算机设备时，就已对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取了防辐射措施，把电磁辐射抑制到最低限度。生产和使用低辐射计算机设备是防止计算机电磁辐射泄密的较为根本的防护措施。Tempest是美国制订的一套保密标准，国外一些先进的工业国家对Tempest技术的应用非常重视，在重要场合使用的计算机设备对辐射的要求都极为严格。如美国军队在开赴海湾战争前线之前，就将所有的计算机更换成低辐射计算机。国外已能生产出系列化的Tempest产品，如Tempest个人计算机、工作站、连接器、打印机、绘图仪、通信终端、视频显示器等。Tempest产品造价非常高，一台Tempest设备要比具有同样性能的设备昂贵3～4倍。

3. 技术标准

目前，国家保密部门已经制订了《电话机电磁泄漏发射限值和测试方法》（BMB—1）、《信息设备电磁泄漏发射限值》（GBB—1）、《使用现场的信息设备电磁泄漏发射检查测试方法和安全判据》（BMB—2）、《处理涉密信息的电磁屏蔽室的技术要求和测试方法》（BMB—3）等4项保密标准，各单位应该对各部门使用的涉密信息设备进行技术检测，由保密部门通过检测仪器进行检测，如果发现问题，及时采取必要的措施堵塞漏洞，防止国家秘密的泄露。



7.6.3 容灾系统建设

1. 容灾系统简介

当计算机信息系统在遭受诸如火灾、水灾、地震、战争或人为破坏等灾难时，计算机系统的硬件、数据、系统和服务都会受到不同程度的破坏。如果灾难发生在通信、金融或军事系统，系统不能及时应付灾难，恢复系统功能，将会造成不可估计的损失。容灾（Disaster Recovery）系统，简称 DR 系统，也称为灾难恢复系统，就是通过特定的容灾机制，能够在各种灾难损害发生后，仍然能够最大限度地保障提供正常应用服务的计算机信息系统。

容灾系统按照所保障的内容分类，可以分为数据级容灾和应用级容灾系统。数据级容灾系统需要保证用户数据的完整性、可靠性和安全性，而对于提供实时服务的信息系统，用户的服务请求在灾难中可能会中断。应用级容灾系统能够提供不间断的应用服务，当发生灾难时客户的服务请求仍然能够透明地毫无觉察地继续运行，保证信息系统提供的服务完整、可靠、安全。

容灾系统按照容灾功能实现的距离远近，又可以分为远程容灾系统和近距容灾系统。远程应用级容灾系统，指距离较远的（至少超过 100km），能够在灾难中提供正常应用服务的计算机信息系统，不仅是数据的动态备份系统，也是应用的动态备份系统，是最能经受灾难考验和最具战略价值的容灾系统，也是实现难度和成本最大的容灾系统。

2. 容灾系统结构模型

容灾系统是对现有应用系统改造，加入容灾功能之后的应用系统，按照软件系统结构，新的容灾系统分为两层，应用系统层和容灾平台层，其结构模型如图 7-14 所示。

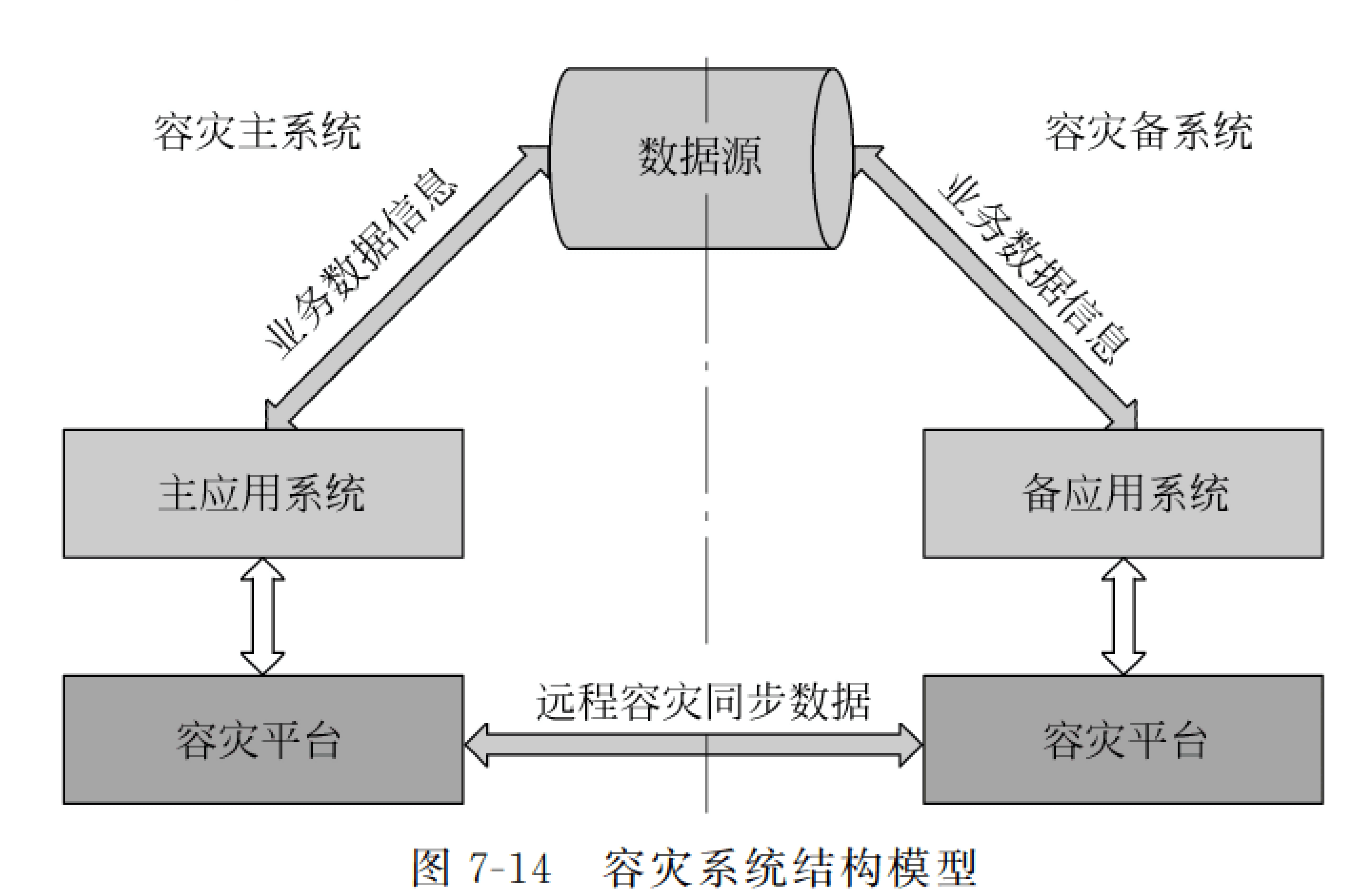


图 7-14 容灾系统结构模型

如图可以看出，容灾系统中的主系统和备系统，两者的结构完全一致，分别由主应用系统和容灾平台构成，应用系统根据输入的业务数据信息完成处理，并且与容灾平台交互信息。主系统的容灾平台根据主备系统一致的要求，产生能够控制主备系统处理结果一致的容灾同步数据，通过容灾平台进行远程传输到备系统的容灾平台，备系统容灾平台完成容灾同步数据的分析和处理，然后控制备系统的应用系统完成相关业务操作。

考虑到业务数据量可能很大并且相对独立，不便通过容灾同步数据传输，因此在数据源的采集过程中，分别发送到容灾主系统和容灾备系统，容灾平台只负责容灾同步数据的交互，减少了主备系统之间的数据交互，特别有利于远程容灾系统，利用少量的容灾同步数据，控制备系统的处理与主系统完全一致，达到容灾备份的目的。

由于该模型采用两套应用系统，使得容灾平台依赖于应用系统，并且建立两套应用系统，使得该系统的成本比较高，实施困难。但是，要保证真正意义上的实时的远程容灾备份功能，使得在主系统出现灾难并且可能是完全损毁或不存在的情况下，备系统能够接替主系统的工作，则必须建立一套与主系统功能完全一致的备系统。

3. 容灾平台

容灾系统实施的关键是容灾平台（Disaster Recovery Platform）的构建。容灾平台完成同步数据的生成、管理、传输及应用系统的同步功能，保障主备系统间的应用程序的同步及备份功能，所提供的功能在主备系统是有所差异的。容灾平台的实施模型如图 7-15 所示。

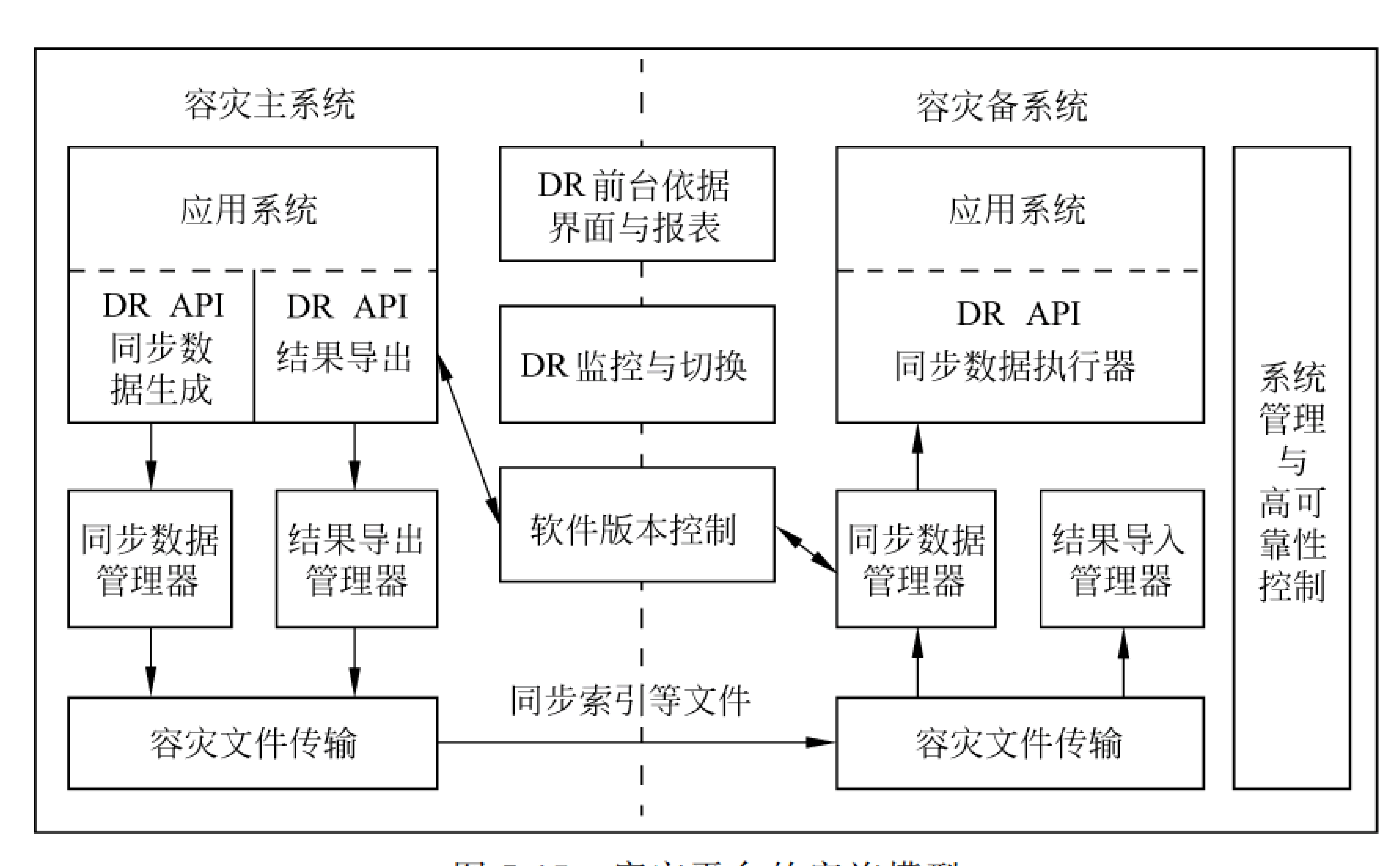


图 7-15　容灾平台的实施模型

在主系统中，应用系统与容灾平台协作，调用容灾平台的应用程序接口(DR API)，获取同步信息，如输入参数、系统时间、环境变量、处理文件名、生成结果等，经 DR 平台将同步数据打包生成同步数据文件，通过同步数据管理器及文件传输系统，将同步信息传输到备系统。

备系统的容灾平台在接收到同步数据信息后，通过同步数据管理器进行解包验证处理，并且按照主系统的处理顺序，交给 DR API 同步索引执行器，备系统应用系统通过 DR API 获得同步信息，执行信息服务处理程序，完成与主系统一致的操作。

考虑到某些数据量较小的结果是无法通过 DR API 的同步索引生成机制获得备份的，就考虑添加 DR API 结果导出功能，应用系统通过 DR API 的结果导出功能，将结果导出后，交给结果导出管理器管理打包，再通过传输系统传送到备系统，备系统的结果导入管理器接收到主系统的导出结果，在备系统进行相应的导入工作，完成主系统关键数据的备份功能。

除了同步数据生成及结果导入导出模块外，还需要考虑主备系统软件版本同步控制、容灾监控与切换以及容灾前台维护界面与报表功能。

综上所述，容灾平台实施模型包括以下几个功能模块：

(1) 容灾应用程序接口(DR API)。即容灾系统开发平台，功能主要包括 IDX 生成和执行 API、容灾结果导出 API，这些 API 需要嵌入到三期的应用程序中去，并且在以后新业务开发过程中都要遵守依据此平台所制订的容灾开发规范，在新业务的应用程序中适当地嵌入 DR API，来保证主备系统处理的同步。

(2) 同步数据管理模块。包括同步数据文件生成(在主系统中根据容灾 API 所产生的同步数据生成同步数据文件以便向备系统传递)，公共参表数据版本管理同步，同步数据解释执行(在备系统中)，业务程序间依赖关系检测等功能。它是容灾平台的核心，负责协调各个子系统，对备系统有调度功能，它负责启动或触发所有的三期需同步的应用程序。

(3) Exporter/Importer 结果导出/导入模块。依 API 导出结果数据生成数据映像文件，从映像文件导入数据库等，作为 DR API 的补充。结果导入也利用同步数据管理器来调度协调主备系统。

(4) 软件版本控制。用于控制和监控容灾系统源代码、执行码的版本，确保主备系统使用相同版本的软件，包括软件的包装、安装和升级等过程的控制。软件版本的更新必须遵循严格的规范。

(5) 容灾前台维护界面。容灾前台维护界面用于配置容灾同步管理平台，使其满足三期系统的容灾需求，并与被应用系统调用的容灾应用程序接口(DR API)相配合。前台维护界面包括应用系统同步数据参数配置，结果导出/导入参数配置，软件版本管理与安装界面等。

(6) 容灾文件传输。容灾文件传输的主要功能包括广域网中转、主备同步信息文件传输。由于备系统需要建立和外部系统的网络连接以及主备系统之间的热线网络，因而在广域网物

理拓扑结构上已经建立了一套备份网络，从而可以在外部系统与主系统之间发生网络传输故障时通过备系统来中转数据，这样可以充分发挥容灾备份的潜力，提高主系统的可靠性、稳定性和及时性。主备同步信息文件传输主要负责将主系统产生的同步数据文件传递到备系统。

（7）系统管理与高可靠性控制。系统操作员可以通过该功能模块管理控制主系统和备系统，诊断故障，保障系统的高可靠性，系统对可预见故障，能够自动修复错误，如果出现较大故障，系统进行高可靠性本地切换或主备系统切换。

7.6.4 CA认证中心建设

1. 什么是CA

CA是认证中心的英文Certification Authority缩写。它为电子商务、电子政务等网络环境中各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理证书；CA对数字证书的签名使得第三者不能伪造和篡改证书。它是电子商务和网上银行交易的权威性、可信赖性及公正性的第三方机构。

2. 什么是PKI

PKI即公钥密码基础设施（Public Key Infrastructure），是利用公钥理论和技术建立的提供安全服务的基础设施，是信息安全技术的核心。由于通过网络进行的电子商务、电子政务、电子事务等活动缺少物理的接触，因而使得用电子方式验证信任关系变得至关重要。而公钥基础设施技术恰好是一种适合电子商务、电子政务、电子事务的密码技术，它能够有效地解决电子活动中的机密性、真实性、完整性、不可否认性和存取控制等安全问题。CA是PKI的核心机构，PKI是CA的关键技术。

3. CA的功能

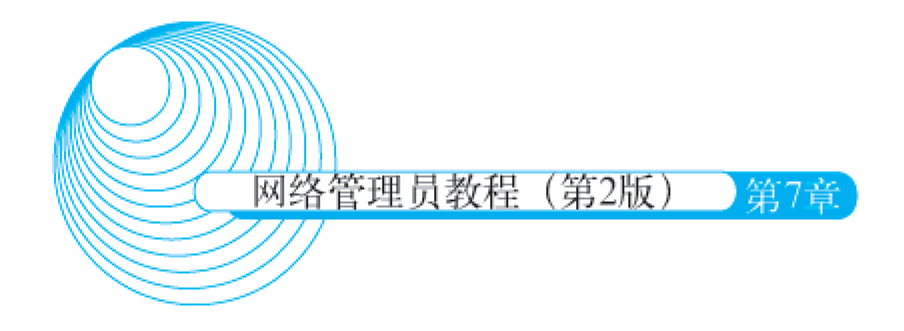
CA认证中心通常采用国内外先进技术，按国际通用标准开发建设，它具有对用户证书的申请、审核、批准、签发证书及证书下载、证书注销、证书更新等证书管理功能。证书符合ITU的X.509国际标准。提供具有世界先进水平的CA认证中心的全部需求。归纳起来，其功能主要包括以下几个方面：

（1）证书的申请。申请方式可分为离线申请方式和在线申请方式。

（2）证书的审批。批准方式可分为离线审核方式和在线审核方式。

（3）证书的发放。发放方式可分为离线方式发放和在线方式发放。

（4）证书的归档。



（5）证书的撤销。

（6）证书的更新。更新方式可分为人工密钥更新和自动密钥更新。

（7）证书废止列表管理(CRL,Certificate Rescind List)。具体包括证书废止原因编码 、CRL的产生及其发布、企业证书及 CRL 的在线服务功能。

（8）CA 本身的管理和 CA 自身密钥的管理。

第8章　网络管理

8.1　网络管理简介

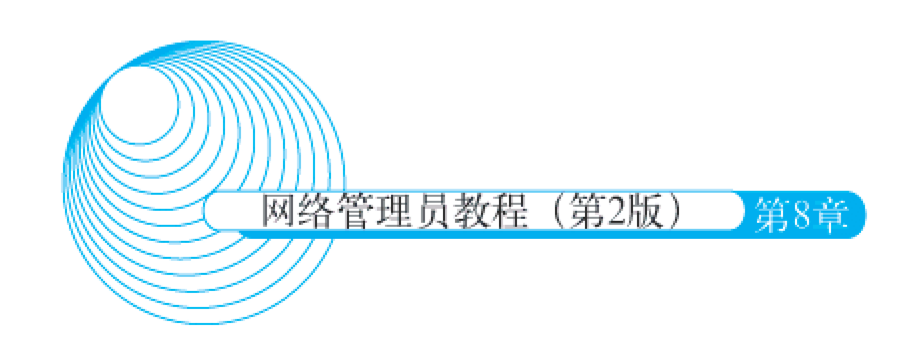
8.1.1　网络管理概述

网络管理是指对网络的运行状态进行监测和控制，使其能够有效、可靠、安全、经济地提供服务。从这个定义可以看出，网络管理包含两个任务：一是对网络的运行状态进行监测，二是对网络的运行状态进行控制。通过监测可以了解当前状态是否正常，是否存在瓶颈和潜在的危机，通过控制可以对网络状态进行合理调节，提高性能，保证服务。监测是控制的前提，控制是监测的结果。由此可见，网络管理具体地说就是网络的监测和控制。

随着网络的发展，规模增大、复杂性增加，以前的网络管理技术已不能适应网络的迅猛发展。特别是这些网络管理系统往往是厂商自己开发的专用系统，很难对其他厂商的网络系统、通信设备和软件等进行管理。这种状况很不适应网络异构互联的发展趋势。尤其是 20 世纪 80 年代初期因特网的出现和发展更使人们意识到了这一点。为此，研发者们迅速展开了对网络管理这门技术的研究，并提出了多种网络管理方案，具有代表性的有 CMIS/CMIP（Common Management Information Service/Protocol）和 SNMP（Simple Network Management Protocol）。

到 1987 年底，管理因特网策略和方向的核心管理机构因特网体系结构委员会（IAB）意识到，需要在众多的网络管理方案中选择适合于 TCP/IP 网络、特别是 Internet 的管理方案。IAB 在 1988 年 3 月的会议上，制订了因特网管理的发展策略，即采用 SGMP 作为短期的因特网的管理解决方案，并在适当的时候转向 CMIS/CMIP。其中，SGMP 是 1986 年 NSF 资助的纽约证券交易所网（NYSERNET，New York Stock Exchange）上开发应用的网络管理工具，而 CMIS/CMIP 是 20 世纪 80 年代中期国际标准化组织（ISO）和国际电话与电报顾问委员会（CCITT）联合制订的网络管理标准。同时，IAB 还分别成立了相应的工作组，对这些方案进行适当的修改，使它们更适合于因特网的管理。这些工作组分别在 1988 年和 1989 年先后推出了 SNMP 和 CMOT（CMIP/CMIS Over TCP/IP）。但实际情况的发展并非如 IAB 计划的那样，SNMP 一推出就得到了广泛的应用和支持，而 CMIS/CMIP 的实现却由于其复杂性和实现代价太高而遇到了困难。当 ISO 不断修改 CMIS/CMIP 使之趋于成熟时，SNMP 在实际应用环境中得到了检验和发展。

1990 年因特网工程任务组（IETF，Internet Engineering Task Force）在因特网标准草案 RFC1157（Request For Comments）中正式公布了 SNMP，1993 年 4 月又在 RFC1441 中发布了 SNMPv2。当 ISO 的网络管理标准终于趋向成熟时，SNMP 已经得到了数百家厂商的支持，其中



包括 IBM、HP、Sun 等许多 IT 界著名的公司和厂商。目前 SNMP 已成为网络管理领域中事实上的工业标准，并被广泛支持和应用，大多数网络管理系统和平台都是基于 SNMP 的。

由于实际应用的需要，对网络管理的研究越来越多，并已成为涉及通信和计算机网络领域的全球性热门课题。国际电气电子工程师协会（IEEE）通信学会下属的网络营运与管理专业委员会（CNOM，Committee of Network Operation and Management），从 1988 年起每两年举办一次网络运营与管理专题讨论会（NOMS，Network Operation and Management Symposium）。国际信息处理联合会（IFIP）也从 1989 年开始每两年举办一次综合网络管理专题讨论会。ISO 还专门设立了一个 OSI 网络管理论坛（OSI/NMF），专门讨论网络管理的有关问题。

8.1.2 网络管理功能

ISO 在 ISO/IEC 7498-4 文档中定义了网络管理的 5 大功能，并被广泛接受。这 5 大功能分别是：

1. 故障管理（Fault Management）

故障管理是网络管理中最基本的功能之一。用户都希望有一个可靠的计算机网络。当网络中某个组成部分发生故障时，网络管理器必须迅速查找到故障并及时排除。故障管理的主要任务是发现和排除网络故障。故障管理用于保证网络资源的无障碍、无错误的运营状态。包括障碍管理、故障恢复和预防保障。障碍管理的内容有告警、测试、诊断、业务恢复、故障设备更换等。预防保障为网络提供自愈能力，在系统可靠性下降，业务经常受到影响的准故障条件下实施。在网络的监测和测试中，故障管理参考配置管理的资源清单来识别网络元素。如果维护状态发生变化，或者故障设备被替换，以及通过网络重组迂回故障时，要与资源 MIB 互通。在故障影响了有质量保证承诺的业务时，故障管理要与计费管理互通，以赔偿用户的损失。

通常不大可能迅速隔离某个故障，因为网络故障的产生原因往往相当复杂，特别是当故障是由多个网络组成部分共同引起的，在此情况下，一般先将网络修复，然后再分析网络故障的原因。分析故障原因对于防止类似故障的再次发生相当重要。网络故障管理包括故障检测、隔离故障和纠正故障 3 个方面，应包括以下典型功能：

（1）维护并检查错误日志；

（2）接受错误检测报告并作出响应；

（3）跟踪、辨认错误；

（4）执行诊断测试；

（5）纠正错误。

对网络故障的检测依据对网络组成部件状态的监测。那些不严重的简单故障通常被记录在错误日志中，并不作特别处理；而严重一些的故障则需要通知网络管理器，即所谓的“警报”。

一般网络管理器应根据有关信息对警报进行处理，排除故障。当故障比较复杂时，网络管理器应能执行一些诊断测试来辨别故障原因。

2．配置管理（Configuration Management）

配置管理是最基本的网络管理功能，负责网络的建立、业务的展开以及配置数据的维护。配置管理功能主要包括资源清单管理、资源开通以及业务开通。资源清单的管理是所有配置管理的基本功能，资源开通是为满足新业务需求及时地配备资源，业务开通是为端点用户分配业务或功能。配置管理建立资源管理信息库（MIB）和维护资源状态，为其他网络管理功能利用。配置管理初始化网络，并配置网络，以使其提供网络服务。配置管理的目的是为了实现某个特定功能或使网络性能达到最优。

配置管理是一个中长期的活动。它要管理的是网络增容、设备更新、新技术的应用、新业务的开通、新用户的加入、业务的撤销、用户的迁移等原因所导致的网络配置的变更。网络规划与配置管理关系密切。在实施网络规划的过程中，配置管理发挥最主要的管理作用。配置管理包括：

（1）设置开放系统中有关路由操作的参数；

（2）被管对象和被管对象组名字的管理；

（3）初始化或关闭被管对象；

（4）根据要求收集系统当前状态的有关信息；

（5）获取系统重要变化的信息；

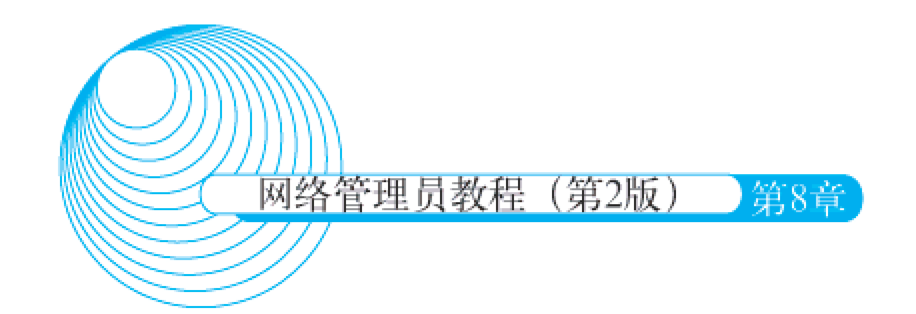
（6）更改系统的配置。

3．计费管理（Accounting Management）

计费管理记录网络资源的使用，目的是控制和监测网络操作的费用和代价。它可以估算出用户使用网络资源可能需要的费用和代价。网络管理员还可规定用户可使用的最大费用，从而控制用户过多占用和使用网络资源。这也从另一方面提高了网络的效率。另外，当用户为了一个通信目的，需要使用多个网络中的资源时，计费管理应可计算总计费用。

计费管理根据业务及资源的使用记录制作用户收费报告，确定网络业务和资源的使用费用，计算成本。计费管理保证向用户无误地收取使用网络业务应交纳的费用，也进行诸如管理控制的直接运用和状态信息提取一类的辅助网络管理服务。一般情况下，收费机制的启动条件是业务的开通。

计费管理的主要目的是正确地计算和收取用户使用网络服务的费用。但这并不是唯一的目的，计费管理还要进行网络资源利用率的统计和网络的成本效益核算。对于以赢利为目的的网络经营者来说，计费管理功能无疑是非常重要的。



在计费管理中，首先要根据各类服务的成本、供需关系等因素制订资费政策，资费政策还包括根据业务情况制订的折扣率。其次要收集计费收据，如使用的网络服务、占用时间、通信距离、通信地点等计算服务费用。通常计费管理包括以下几个主要功能：

(1) 计算网络建设及运营成本。主要成本包括网络设备器材成本、网络服务成本、人工费用等。

(2) 统计网络及其所包含的资源的利用率。为确定各种业务各种时间段的计费标准提供依据。

(3) 联机收集计费数据。这是向用户收取网络服务费用的根据。

(4) 计算用户应支付的网络服务费用。

(5) 账单管理。保存收费账单及必要的原始数据，以备用户查询和置疑。

4. 性能管理(Performance Management)

性能管理的目的是维护网络服务质量(QoS)和网络运营效率。为此，性能管理要提供性能监测功能、性能分析功能以及性能管理控制功能。同时，还要提供性能数据库的维护以及在发现性能严重下降时启动故障管理系统的功能。

网络服务质量和网络运营效率有时是相互制约的。较高的服务质量通常需要较多的网络资源(带宽、CPU 时间等)，因此在制订性能目标时要在服务质量和运营效率之间进行权衡。在网络服务质量必须优先保证的场合，就要适当降低网络的运营效率指标；相反，在强调网络运营效率的场合，就要适当降低服务质量指标。但一般在性能管理中，维护服务质量是第一位的。

性能管理估价系统资源的运行状况及通信效率等系统性能。其功能包括监视和分析被管网络及其所提供服务的性能机制。性能分析的结果可能会触发某个诊断测试过程或重新配置网络以维持网络的性能。性能管理收集分析有关被管网络当前状况的数据信息，并维持和分析性能日志。一些典型的功能包括：

(1) 收集统计信息；

(2) 维护并检查系统状态日志；

(3) 确定自然和人工状况下系统的性能；

(4) 改变系统操作模式以进行系统性能管理的操作。

5. 安全管理(Security Management)

安全性一直是网络的薄弱环节之一，而用户对网络安全的要求又相当高，因此网络安全管理非常重要。网络中主要有以下几大安全问题：网络数据的私有性(保护网络数据不被侵入者非法获取)；授权(防止侵入者在网络上发送错误信息)；访问控制(控制对网络资源的访问)。

安全管理采用信息安全措施保护网络中的系统、数据以及业务。安全管理与其他管理功能

有着密切的关系。安全管理要调用配置管理中的系统服务对网络中的安全设施进行控制和维护。当网络发现安全方面的故障时，要向故障管理通报安全故障事件以便进行故障诊断和恢复。安全管理功能还要接收计费管理发来的与访问权限有关的计费数据和访问事件通报。

安全管理的目的是提供信息的隐私、认证和完整性保护机制，使网络中的服务、数据以及系统免受侵扰和破坏。一般的安全管理系统包含以下 4 项功能：

(1) 风险分析功能；

(2) 安全服务功能；

(3) 告警、日志和报告功能；

(4) 网络管理系统保护功能。

8.1.3 网络管理基本模型

在网络管理中，一般采用网络管理者——网管代理模型，如图 8-1 所示。网络管理模型的核心是一对相互通信的系统管理实体。它采用一个独特的方式使两个管理进程之间相互作用。即，管理进程与一个远程系统相互作用，来实现对远程资源的控制。在这种简单的体系结构中，一个系统中的管理进程担当管理者角色，而另一个系统中的对等实体担当代理者角色，代理者负责提供对被管对象的访问。前者被称为网络管理者，后者被称为网管代理。不论是 OSI 的网络管理，还是 IETF 的网络管理，都认为现代计算机网络管理系统基本上由以下 4 个要素组成：

(1) 网络管理者(Network Manager)；

(2) 网管代理(Managed Agent)；

(3) 网络管理协议(Network Management Protocol)；

(4) 管理信息库(MIB，Management Information Base)。

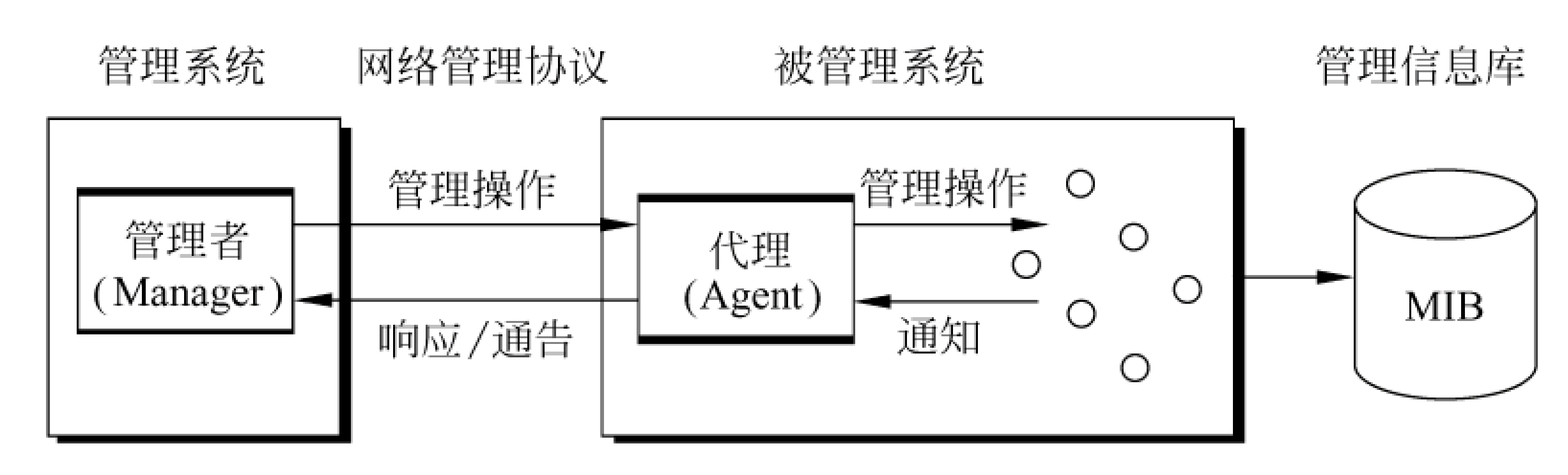
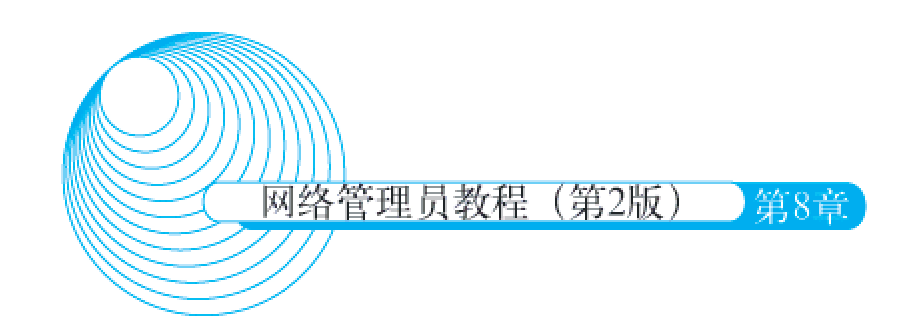


图 8-1　网络管理的基本模型

网络管理者(管理进程)驻留在管理工作站上，管理工作站可以是工作站、微机等，一般位于网络系统的主干或接近于主干的位置，它负责发出管理操作的指令，并接收来自被管代理的信息。网络管理者通过各网管代理对网络内的各种设备、设施和资源实施监视和控制。网络管理者收集到的信息将被用于确定独立的网络设备、部分网络或整个网络运行的状态是否正常。网管代理是一个软件模块，它驻留在被管设备上，负责管理指令的执行，并且以通知的形式向网络



管理者报告被管对象发生的一些重要事件。网管代理具有两个基本功能：一是从 MIB 中读取各种变量值；二是在 MIB 中修改各种变量值。MIB 是被管对象结构化组织的一种抽象。它是一个概念上的数据库，由管理对象组成，各个网管代理管理 MIB 中属于本地的管理对象，各管理网管代理控制的管理对象共同构成全网的管理信息库。网络管理协议是最重要的部分，它定义了网络管理者与网管代理间的通信方法，规定了管理信息库的存储结构、信息库中关键词的含义以及各种事件的处理方法。目前有影响的网络管理协议是 SNMP 和 CMIS/CMIP。它们代表了目前两大网络管理解决方案。

另外，需要说明的是在系统管理模型中，管理者角色与网管代理角色不是固定的，而是由每次通信的性质所决定。担当管理者角色的进程向担当网管代理角色的进程发出操作请求，担当网管代理角色的进程对被管对象进行操作并将被管对象发出的通报传向管理者。

8.2 简单网络管理协议

8.2.1 SNMP 概述

SNMP 是由一系列协议组和规范组成，它们提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 的体系结构分为 SNMP 管理者（SNMP Manager）和 SNMP 代理者（SNMP Agent），每一个支持 SNMP 的网络设备中都包含一个网管代理，网管代理随时记录网络设备的各种信息，网络管理程序再通过 SNMP 通信协议收集网管代理所记录的信息。从被管理设备中收集数据有两种方法：一种是轮询方法，另一种是基于中断的方法。

SNMP 使用嵌入到网络设施中的代理软件来收集网络的通信信息和有关网络设备的统计数据。代理软件不断地收集统计数据，并把这些数据记录到一个管理信息库中。网管员通过向代理的 MIB 发出查询信号可以得到这些信息，这个过程就叫轮询。为了能够全面地查看一天的通信流量和变化率，管理人员必须不断地轮询 SNMP 代理，每分钟就轮询一次。这样，网管员可以使用 SNMP 来评价网络的运行状况，并分析出通信的趋势。例如，哪一个网段接近通信负载的最大能力或正在使用的通信出错等。先进的 SNMP 网管站甚至可以通过编程来自动关闭端口或采取其他矫正措施来处理历史的网络数据。

如果只是用轮询的方法，那么网络管理工作站总是在控制之下。但这种方法的缺陷在于信息的实时性，尤其是错误的实时性。多长时间轮询一次、轮询时选择什么样的设备顺序都会对轮询的结果产生影响。轮询的间隔太小，会产生太多不必要的通信量；间隔太大，而且轮询时顺序不对，那么关于一些大的灾难性事件的通知又会太慢，这就违背了积极主动的网络管理目的。与之相比，当有异常事件发生时，基于中断的方法可以立即通知网络管理工作站，实时性很强。但这种方法也有缺陷。产生错误或自陷需要系统资源，如果自陷必须转发大量的信息，那么被管理设备可能不得不消耗更多的事件和系统资源来产生自陷，这将会影响到网络管理的主要

功能。

结果，将以上两种方法结合起来，就形成了陷入制导轮询方法。一般来说，网络管理工作站轮询在被管理设备中的代理来收集数据，并且在控制台上用数字或图形的表示方法来显示这些数据。被管理设备中的代理可以在任何时候向网络管理工作站报告错误情况，而并不需要等到管理工作站为获得这些错误情况而轮询它的时候才报告。

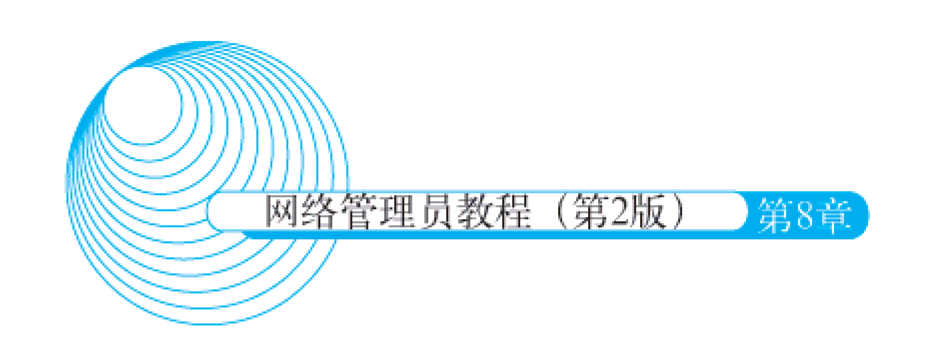
简单网络管理协议（SNMP）已经成为事实上的标准网络管理协议。由于 SNMP 首先是 IETF 的研究小组为了解决在因特网上的路由器管理问题提出的，因此许多人认为 SNMP 只能在 IP 上运行，但事实上，目前 SNMP 已经被设计成与协议无关的网管协议，所以它在 IP、IPX、AppleTalk 等协议上均可以使用。

SNMP 在计算机网络中应用非常广泛，虽已成为事实上的计算机网络管理的标准，但是 SNMP 还有许多自身难以克服的缺点：SNMP 不适合管理真正的大型网络，因为它是基于轮询机制的，在大型网络中效率很低。轮询有两个明显的缺点：一是没有伸缩性。在大型网络中，轮询会产生巨大的网络管理通信量，因而会导致通信拥挤情况的发生；二是网络管理器负担加重。SNMP 轮询中收集数据的任务是由网络管理器完成的，通常管理器在监控 3 个以上网段时，会因负载加重而不能完成任务；SNMP 的 MIB 模型不适合比较复杂的查询，不适合大量数据的查询；SNMP 的陷入（trap）是无确认的，这样不能确保将那些非常严重的告警发送到管理者；SNMP 的安全管理较差，缺乏安全措施，无数据源认证、不能防止偷听、SNMP 的团体名在对付日益猖獗的网络入侵和窃听方面无能为力。

随着网络的发展，对 SNMP 的改进与增强也在进行，RMON（远程网络监视）、SNMPv2c 以及 SNMPv3 是 SNMP 发展史上的重要阶段。RMON 的出现是为了适应网络管理应能支持新的分布式结构、提供更高性能的应用和面对更多的用户的需求而出现的。IETF 于 1991 年 11 月公布的 RFC1271 定义了 RMON MIB，对 SNMP 轮询的弊端进行了弥补，扩充了管理信息库 MIB－2，可以提供有关互联网管理的主要信息，在不改变 SNMP 协议的条件下增强了网络管理的功能，进一步解决了 SNMP 在日益扩大的分布式网络中所面临的局限性。可以说 RFC1271 公布是互联网管理上的一个巨大进步。

SNMPv2 相对 SNMPv1 着重在管理信息结构、管理器之间的通信能力和协议操作 3 个方面进行了改进。但是该版本仍然存在安全缺陷，为此，只是把新增加的功能作为一个新的版本发布，该版本保留了 SNMPv1 的报文封装格式，因此，该版本被命名为基于团体名的 SNMP（Community-based SNMP），即 SNMPv2c。

SNMPv2c 功能增强了，但是安全性能仍没有得到改善，继续使用 SNMPv1 的基于团体名的明文密钥的身份验证方式。IETF SNMPv3 工作组于 1998 年元月提出了互联网建议 RFC 2271-2275，正式形成了 SNMPv3，这一系列文件定义了包含 SNMPv1、SNMPv2 所有功能在内的体系框架和包含验证服务和加密服务在内的全新的安全机制，同时还规定了一套专门的网络安全和



访问控制规则。可以说，SNMPv3 是在 SNMPv2 基础之上增加了安全和管理机制。

8.2.2 管理信息库

计算机网络管理涉及到网络中的各种资源，包括两大类：硬件资源和软件资源。硬件资源是指物理介质、计算机设备和网络互连设备。物理介质通常是物理层和数据链路层设备，如网卡、双绞线、同轴电缆等；计算机设备包括处理机、打印机和存储设备及其他计算机外围设备；常用的网络互连设备有中继器、网桥、路由器、网关等。软件资源主要包括操作系统、应用软件和通信软件。通信软件是指实现通信协议的软件，例如在 FDDI、ATM 和 FR 这些主要依靠软件的网络中就大量采用了通信软件。另外，软件资源还有路由器软件、网桥软件等。

网络环境下资源的表示是网络管理的一个关键问题。目前一般采用“被管对象（Managed Object）”来表示网络中的资源。被管对象的集合被称作 MIB，即管理信息库，所有相关的网络被管对象信息都放在其中。不过应当注意的是，MIB 仅是一个概念上的数据库，在实际网络中并不存在一个这样的库。目前网络管理系统的实现主要依靠被管对象和 MIB，所以它们是网络管理中非常重要的概念。

MIB 是一个信息存储库，是网络管理系统中的一个非常重要的部分。MIB 定义了一种对象数据库，由系统内的许多被管对象及其属性组成。通常，网络资源被抽象为对象进行管理。对象的集合被组织为 MIB。MIB 作为设在网管代理处的管理站访问点的集合，管理站通过读取 MIB 中对象的值来进行网络监控。管理站可以在网管代理处产生动作，也可以通过修改变量值改变网管代理处的配置。

MIB 中的数据可大体分为 3 类：感测数据、结构数据和控制数据。感测数据表示测量到的网络状态。感测数据是通过网络的监测过程获得的原始信息，包括节点队列长度、重发率、链路状态、呼叫统计等。这些数据是网络的计费管理、性能管理和故障管理的基本数据；结构数据描述网络的物理和逻辑构成。对应感测数据，结构数据是静态的（变化缓慢的）网络信息，它包括网络拓扑结构、交换机和中继线的配置、数据密钥、用户记录等。这些数据是网络的配置管理和安全管理的基本数据；控制数据存储网络的操作设置。控制数据代表网络中那些可以调整参数的设置，如中继线的最大流、交换机输出链路业务分流比率、路由表等。控制数据主要用于网络的性能管理。

在现代网络管理模型中，管理信息库是网络管理系统的核心。网络操作员在管理网络时，只与 MIB 打交道，当他要对网络功能进行调整时，只须更新数据库中对应的数据即可，实际对物理网络的操作由数据库系统控制完成。现在有几种已经定义的通用的标准管理信息库，其中使用最广泛、最通用的 MIB 是 MIB-II。

8.2.3 SNMP 操作

实际的网络都是由多个厂家生产的各种设备组成的，主机可能是 SPARC 工作站或 PC 机，

路由器可能来自于 Cisco、3COM 或国产路由器 SED—08。要使网络管理者与不同种类的被管设备通信，就必须以一种与厂家无关的标准方式精确定义网络管理信息。SNMP 管理体系结构由管理者（管理进程）、网管代理和管理信息库（MIB）3 部分组成，该体系结构的核心是 MIB，MIB 由网管代理维护而由管理者读写。管理者是管理指令的发出者，这些指令包括一些管理操作。管理者通过各设备的网管代理对网络内的各种设备、设施和资源实施监视和控制。网管代理负责管理指令的执行，并且以通知的形式向管理者报告被管对象发生的一些重要事件。代理具有两个基本功能：从 MIB 中读取各种变量值；在 MIB 中修改各种变量值。

SNMP 模型采用 ASN.1 语法结构描述对象以及进行信息传输。按照 ASN.1 命名方式，SNMP 代理维护的全部 MIB 对象组成一棵树（即 MIB-II 子树），如图 8-2 所示。理解对象标识符（OID，Object Identifier）的概念及表示方法非常重要，对象的标识，即对象的名字。SMI 采用的是层次型的对象命名规则，所有对象构成一颗命名树，连接从树根节点至对象所在节点路径上所有节点标识便构成了该对象的对象标识符。

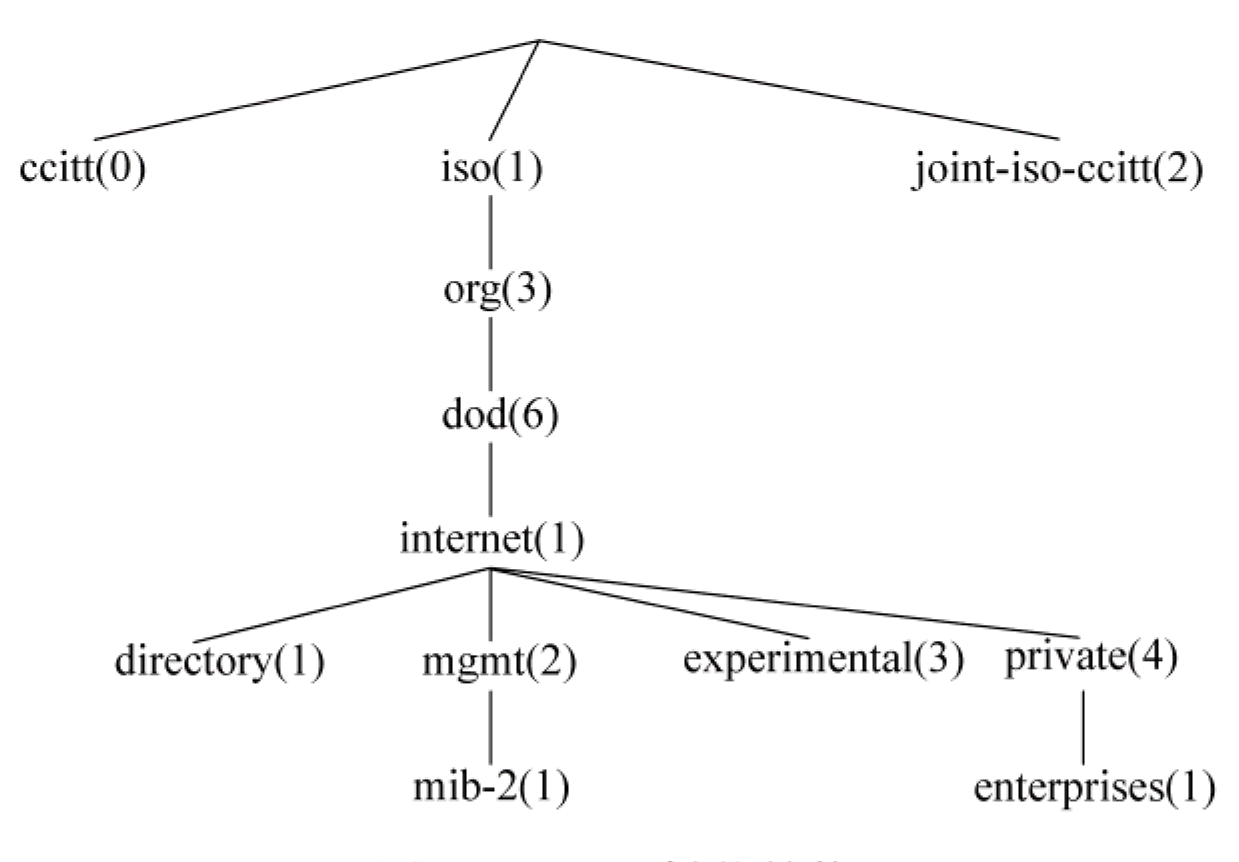


图 8-2　MIB 树状结构

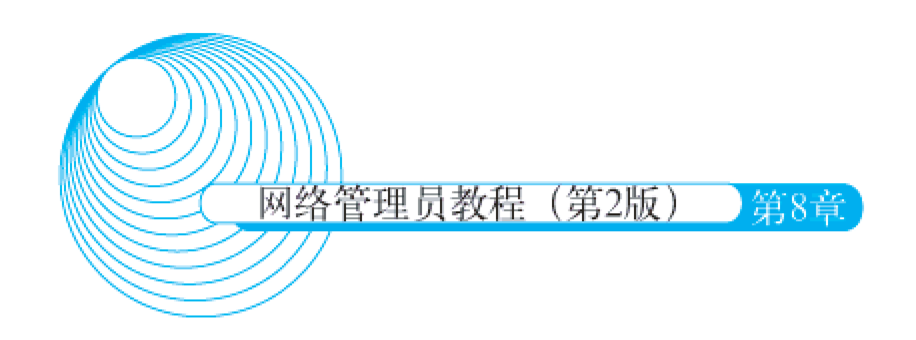
命名树来源于 OSI 的定义，它具有从根开始的严格分层化结构，管理树的分支和叶子是用数字和名字两种方式显示的。数字化编码是机器可读的，名字显示则更适合于人的眼睛并帮助用户寻找穿过错综复杂分支的路径。在树中通向一个节点或叶子的路径是用对象标识符表示的。树的各个分支是用数值表示的，因此对象标识符就构成了一个整数序列，中间是以"."号间隔而成的。

例如，MIB 对象 sysName 对象标识符可以写成如下两种形式：

- iso.org.internet.mgmt.mib-2.system.sysName
- 1.3.6.1.2.1.1.5

可以看出使用数字形式更易于内部存储和处理，并且都有共同的前缀 1.3.6.1。

实际上，SNMP 报文都是采用数字形式的对象标识符，并且为了节省计算和存储空间，内部



处理时省略共同的前缀。

mib-2 管理对象的共同前缀是：1.3.6.1.2.1；企业管理对象的前缀是：1.3.6.1.4.1。

SNMP 定义的管理对象全部在节点 internet 下，internet 的对象标识符是：

internet OBJECT IDENTIFIER::={iso(1) org(3) dod(6) 1}

因此 SNMP 管理对象的对象标识符都是以前缀 1.3.6.1 开始，所以在定义 MIB 的 RFC 中都省略了这一前缀，而以 internet 作为默认的公共前缀，对象标识符简记为父节点的名字标识和本节点的数字标识，如下所示。

```
mgmt OBJECT IDENTIFIER::={internet 2}
mib-2 OBJECT IDENTIFIER::={mgmt 1}
system OBJECT IDENTIFIER::={mib-2 1}
sysName OBJECT IDENTIFIER::={system 5}
```

在传输各类数据时，SNMP 协议首先要把内部数据转换成 ASN.1 语法表示，然后发送出去，另一端收到此 ASN.1 语法表示的数据后也必须首先变成内部数据表示，然后才执行其他的操作，这样就实现了不同系统之间的无缝通信。

IETF RFC1155 的 SMI 规定了 MIB 能够使用的数据类型及如何描述和命名 MIB 中的管理对象类。SNMP 的 MIB 仅仅使用了 ASN.1 的有限子集。它采用了以下四种简单类型数据：INTEGER，OCTET STRING，NULL 和 OBJECT IDENTIFER 以及两个构造类型数据 SEQUENCE 和 SEQUENCE OF 来定义 SNMP 的 MIB。所以，SNMP MIB 仅仅能够存储简单的数据类型：标量型和二维表型。SMI 采用 ASN.1 描述形式，定义了因特网 6 个主要的管理对象类：网络地址、IP 地址、时间标记、计数器、计量器和非透明数据类型。SMI 采用 ASN.1 中的宏的形式来定义 SNMP 中对象的类型和值。

SNMP 实体不需要在发出请求后等待响应到来，是一个异步的请求/响应协议。SNMP 仅支持对管理对象值的检索和修改等简单操作，具体讲，支持下列 4 种操作。

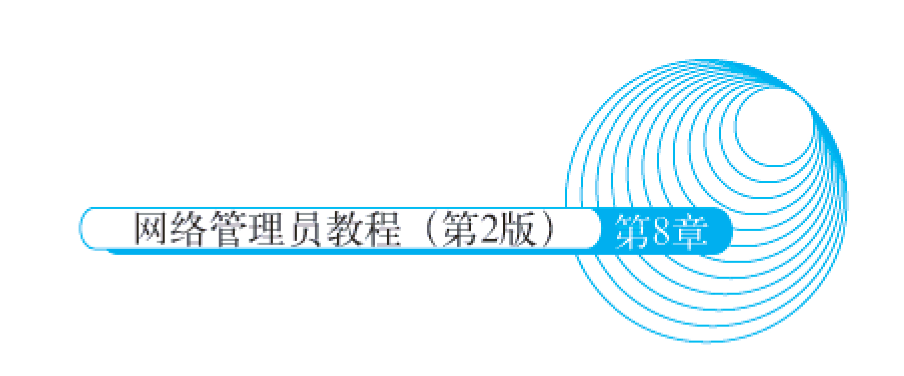
(1) get：用于获取特定对象的值，提取指定的网络管理信息。

(2) get-next：通过遍历 MIB 树获取对象的值，提供扫描 MIB 树和依次检索数据的方法。

(3) set：用于修改对象的值，对管理信息进行控制。

(4) trap：用于通报重要事件的发生，代理使用它发送非请求性通知给一个或多个预配置的管理工作站，用于向管理者报告管理对象的状态变化。

以上 4 个操作中，前 3 个是请求由管理者发给代理，需要代理发出响应给管理者，最后一个则是由代理发给管理者，但并不需要管理者响应。其中，set 操作多数厂商在实现时都废除了该命令，原因是 SNMPv1 的安全性较差。



8.3 网络管理系统

8.3.1 网络管理系统概述

通过前面的学习，读者明白了网络管理的概念、网络管理采用的协议以及网络管理的体系结构（管理站和代理模型）。那么网络管理的最终目标通过什么实现呢？是通过网络管理系统，也就是要通过一个实施网络管理功能的应用系统来实现。随着信息社会对网络的依赖性越来越强，网络管理系统作为附加在业务网这一裸网上的支撑系统，受到了前所未有的重视。对于网络管理员来说，如何有效地管理网络，如何为现有网络规划设计网络管理系统（NMS，Network Management System）已变得尤为迫切。

网络管理系统是用来管理网络、保障网络正常运行的软件和硬件的有机组合，是在网络管理平台的基础上实现的各种网络管理功能的集合，包括故障管理、性能管理、配置管理、安全管理和计费管理等功能。网络管理系统提供的基本功能通常包括：网络拓扑结构的自动发现、网络故障报告和处理、性能数据采集和可视化分析工具、计费数据采集和基本安全管理工具。通过网络管理系统提供的管理功能和管理工具，网络管理员就可以完成日常的各种网络管理任务了。

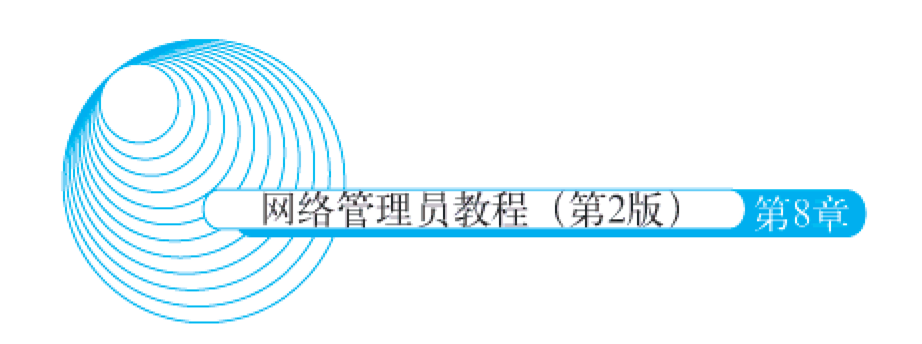
虽然网络管理系统是用来管理网络、保障网络正常运行的关键手段，但在实际应用中，并不能完全依赖于现成的网管产品，由于网络系统复杂多变，现成的产品往往难以解决所有的网管问题。一项权威调查显示，真正直接使用现有的成熟的商业化管理系统的单位仅占受调查单位总数的18%，其余大部分是在现有的网络管理平台上二次开发的系统。也就是说一个好的网络管理系统建设是离不开自主开发的。换句话说，一个成功实用的网络管理系统建设经常伴随着在现有的网络管理平台上进行二次开发的过程。具体地讲，开发设计网络管理系统时，要重点处理好以下问题。

（1）网络管理的跨平台性。当前的网络管理一般都是基于一种专用的硬件和软件管理平台，对网络管理人员的要求很高。但随着Java语言的出现和广泛使用，为开发一种跨平台的网络管理提供了可能。

（2）网络管理的分布式特性。当前的网络管理一般都是集中式管理，既不灵活，也不方便。随着Client/Server计算机模式的广泛应用，如何有效地利用Client/Server结构的特性去实现网络管理的分布式特性，也是一个急需解决的问题。

（3）网络管理的安全特性。安全性问题是网络管理面对的主要挑战。早期的SNMP版本安全性有限，后期版本有了很大的加强。如何在保证网络管理简单性的前提下真正实现安全管理，也是一个不容忽视的问题。

（4）新兴网络模式的管理。随着交换型局域网、虚拟局域网（VLAN）、虚拟专网（VPN）的广



泛使用，如何有效地管理这些网络，是摆在网络管理员面前的一个现实问题。

（5）异种网络设备的管理。现有的网络管理软件大都具有局限性，对不同厂家的不同网络设备的统一管理能力不强。如何将不同厂家的网络设备统一管理起来，也是一个值得思考的问题。

（6）基于 Web 的网络管理。现行标准并不适合服务器响应异步通信。使用 CGI 通过 Web 去集成各设备供应商的管理应用也会遇到一些问题。如何结合 Browser/Server 计算技术开发出基于 Web 的网络管理系统，给网络管理集成技术提出了新的挑战。

8.3.2 HP OpenView

1. HP OpenView 简介

HP OpenView 是一个具有战略性意义的产品，它集成了网络管理和系统管理双方的优点，并把它们有机地结合在一起，形成一个单一而完整的管理系统，从而使企业在急速发展的因特网时代取得辉煌成功，立于不败之地。在 E-Services（电子化服务）的大主题下，OpenView 系列产品包括了统一管理平台、全面的服务和资产管理、网络安全、服务质量保障、故障自动监测和处理、设备搜索、网络存储、智能代理、因特网环境的开放式服务等丰富的功能特性。

HP 公司是最早开发网络管理产品的厂商之一。OpenView 是 HP 公司的旗舰软件产品，已成为网络管理平台的典范，有无数的第三方厂商在 OpenView 的平台上开发网络管理的应用。OpenView 解决方案实现了网络运作从被动无序到主动控制的过渡，使网络管理部门及时了解整个网络当前的真实状况，实现主动控制，而且 OpenView 解决方案的预防式管理工具临界值设定与趋势分析报表，可以让 IT 部门采取更具预防性的措施，以保障管理网络的健全状态。如图 8-3 所示的就是 HP OpenView 的故障诊断模块实现的图形化的端到端网络路径的分析结果。简单地说，OpenView 解决方案是从用户网络系统的关键性能入手，帮助其迅速地控制网络，然后还可以根据需要增加其他解决方案。

需要明确的是 HP OpenView 不是一个特定的产品，而是一个产品系列，它包括一系列管理平台，一整套网络和系统管理应用开发工具。OpenView 是管理多厂商网络设备和系统的战略平台，通过集成多厂商网络设备和系统管理产品，为用户的网络、系统、应用程序和数据库管理提供了统一的解决方案。

2. HP OpenView 管理框架

HP OpenView 解决方案框架为最终用户和应用程序开发商提供了一个基于通用管理过程的体系结构，可为用户提供集成网络、系统、应用程序和适合多用户分布式计算环境的数据库管理。第三方的解决方案可以很容易地集成到 OpenView 系统框架中，为用户和应用开发商提供

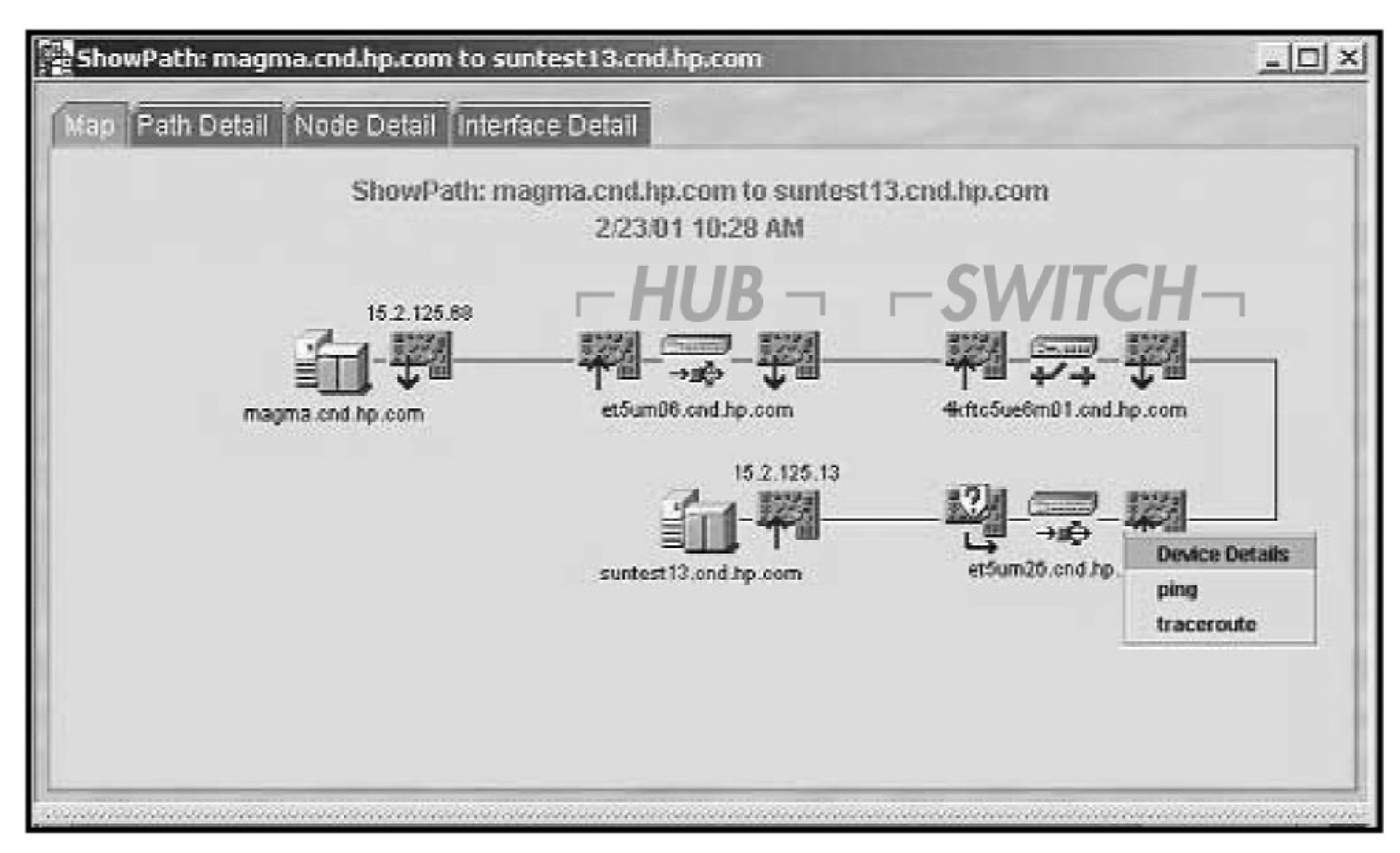


图 8-3　HP OpenView 路径的分析显示结果

一个灵活的解决方案，以适应不断增长的、多厂商产品混杂的、分布式企业计算环境。OpenView 管理框架如图 8-4 所示。

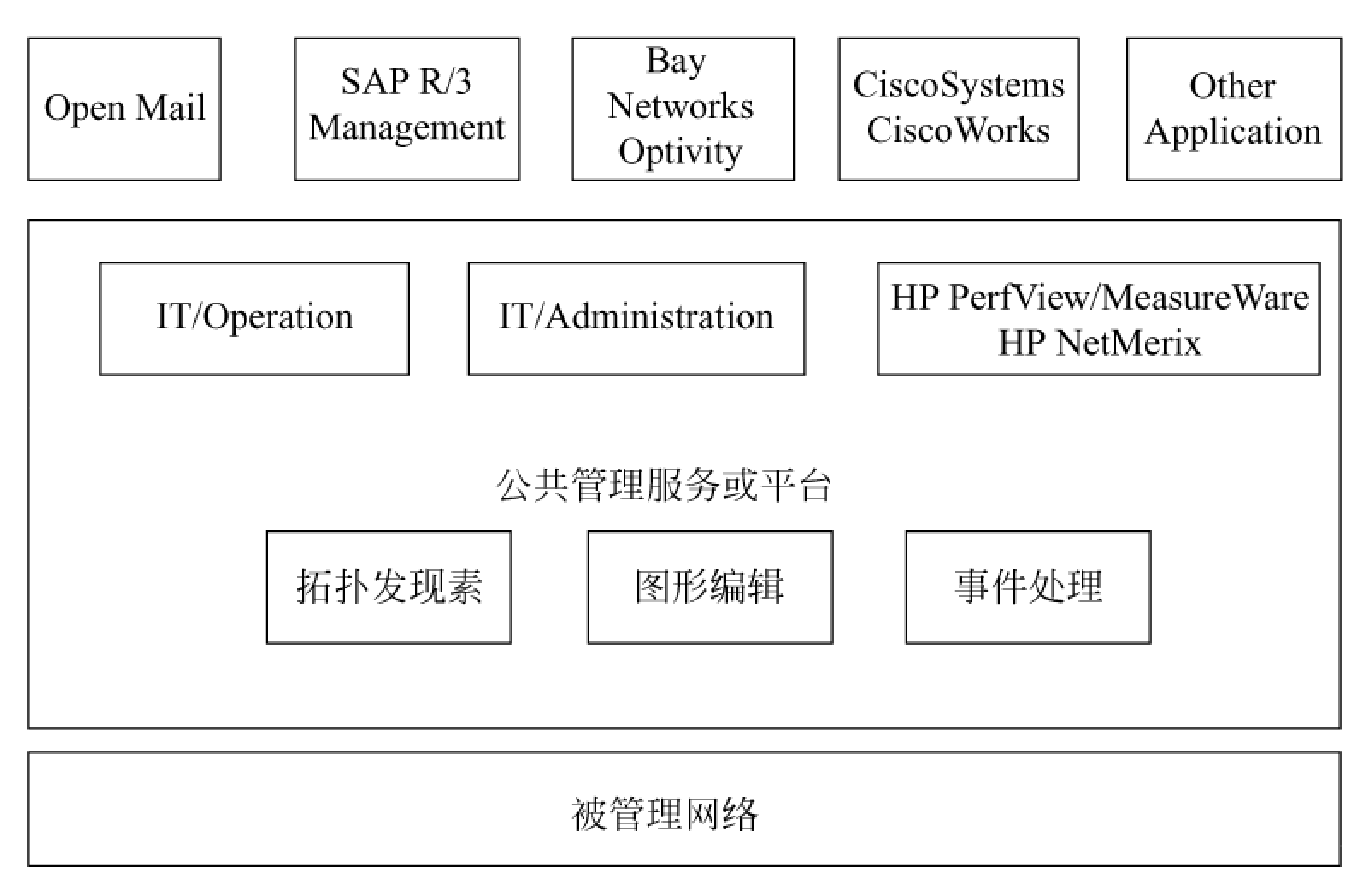
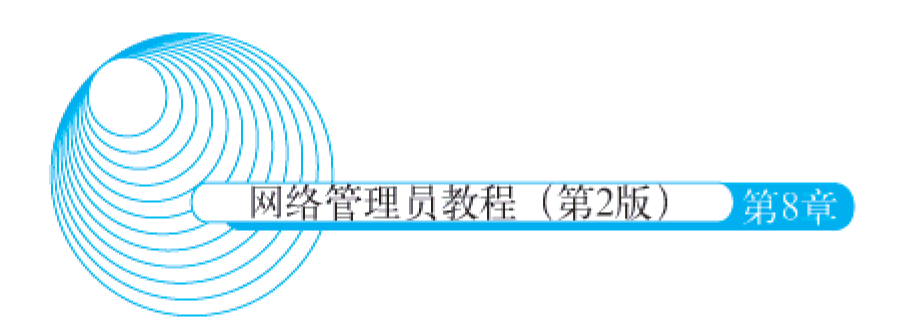


图 8-4　HP OpenView 管理框架



HP OpenView 管理框架包括以下 4 个部件：

（1）用于网络管理的网络节点管理器；

（2）用于操作和故障管理的 IT/Operation；

（3）用于配置和变化管理的 IT/Administration；

（4）用于资源和性能管理的 HP PerfView/MeasureWare 和 HP NetMerix。

3. Network Node Manager

网络对现代企业来说像“血脉”一样重要。一旦网络瘫痪，后果不堪设想。所以，企业必须主动管理网络，以便使网络能够全天候正常运作，只进行被动的网络管理是不能满足可用性要求的。同时，企业还必须管理不断变化的技术，不断适应网络的动态发展，并将各种网络环境集成在一起。HP OpenView 不但意识到了这些问题，还开发出了更强大的网络管理器（NNM，Network Node Manager）来解决这些问题。这种先进的管理解决方案能帮助企业主动管理网络环境，并不断扩展和更新基础设施。

HP OpenView 的 NNM，以其强大的功能、先进的技术、多平台适应性等特点，在全球网络管理领域得到了广泛的应用。NNM 是 HP OpenView 管理框架的基石，是第三方开发和发布网络管理应用系统的网络管理平台，也是最终用户监控和管理 TCP/IP 网络的解决方案。无论是一个小的工作组还是一个校园网，或者是一个分布式多厂商网络环境的大型企业网，NNM 都能以高度的自动化监控整个网络环境。NNM 可以通过 IP 地址、IPX 地址和 MAC 地址发现网络设备，能够运行 SNMP、HTTP 协议的网络设备或 Web 服务器。NNM 还提供了一个图形界面的 SNMP 管理应用，能够支持故障管理、配置管理和性能管理。

NNM 是 OpenView 家族中的主力网络管理系统软件。NNM 的分布式发现与监控机制，允许把处理程序就近安装于用户所处环境的本地域。通过部署多套 NNM，系统管理员就可以通过采集器与管理器管理企业的 IT 环境。采集器与管理器均可使用全版 NNM（不限管理节点数）或简版 NNM（不超过 100 个管理节点），这样一个可伸缩的解决方案可以适应不同规模网络与组织需要，可减少网络流量，从而最大限度地节约网络带宽，把带宽留给真正需要传送的商用信息。NNM 可以成功地监测和控制计算环境，它还可提供一套有力的工具，以便管理从工作组到整个企业的分布式多厂商的网络与系统。NNM 可以用来处理各种技术、应用以及用于建立现在或未来的、本地或全球性的网络设备。它能够为用户节省网络资产，并最大限度地利用已有资源。

特别需要指出的是，2004 年 3 月发布的 HP OpenView Network Node Manager 7.01 开始推出了中文版，它更加易于部署和操作，非常灵活。OpenView NNM 7.0.1 中文版基于 Web 的报告提供了有关网络性能、可用性、库存和异常情况的趋势。对这些历史数据进行分析可以清楚地了解网络中各种设备的状况，从而使网络管理员能够在网络发生故障前采取前瞻性预防

措施。OpenView NNM 7.01 中文版还能够把拓扑、事件和 SNMP 收集的数据都存储在一个外部数据库中，以便于进一步进行分析。此外，OpenView NNM 7.01 中文版能够在监控和管理关键网元的同时，定期进行关键业务网络管理信息的备份。它甚至还可以进行自我监控以确保正常运行和工作，从而保证用户的网络得到不间断的监控，持续可用和正常运行。

8.3.3 Sun Net Manager

Sun 公司的 Net Manager 是 Sun 平台上杰出的网络管理软件，有众多第三方的支持，可与其他管理模块连用，可管理更多的异构环境。尤其在国内的电信网络管理领域中有十分广泛的应用。

Sun NetManager 的分布式结构和协同式管理独树一帜。Sun NetManager 具有如下特点。

(1) 分布式管理。Sun Net Manager 是基于分布式的管理结构，有 3 种分布式管理模式：外部到中央的管理方式、分级的管理方式、协同的管理方式。这种分布式管理模式将管理处理的负载分散到网络上，不仅减少了作为管理者主机的负担，而且降低了网络带宽的开销，为用户提供了管理来自不同厂商的、规模和复杂程序可变的网络及系统的能力。

(2) 协同管理。Sun Net Manager 工具和 Cooperative Console 工具共同实现了协同管理。协同管理将一个小型企业网管按其业务组织或地域分为若干区，每个区都有自己独立的网管系统。但有关区之间可以互相作用，区与区之间的关系可根据实际需要灵活配置。

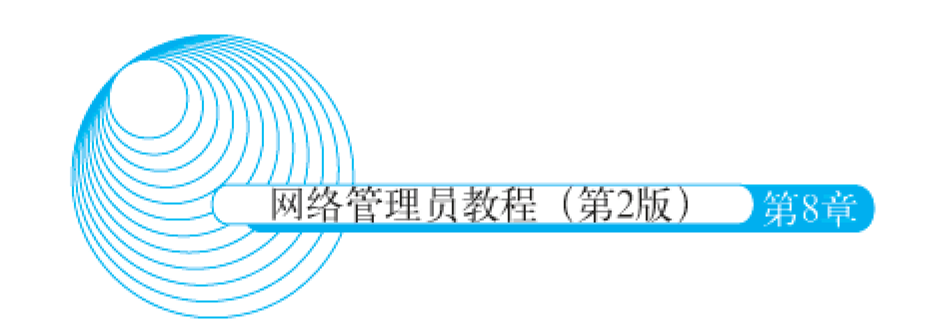
(3) 全面支持 SNMP。Sun Net Manager 包括了所有基本的 SNMP 机制，同时还支持 SNMPV2，而且允许配置 SNMP 陷阱(trap)为不同的优先等级，在网络中出现故障时，能够按优先级传送到其他 Solstice 或非 Solstice 的平台上。

(4) 具有较强的安全性。Sun Net Manager 在配置 Cooperative Console 时，提供了 ACL 以保证被授权接受管理数据的用户能够得到相关信息。另外 Cooperative Console 还提供了只读控制台的功能，使得一般的网管人员只能在只读方式下操作，不能增加/移动/删除网络元素。

(5) 具有强大的应用接口。Sun Net Manager 既提供了用户工具，又提供了开发工具，以补充 Sun Net Manager 中包含的用户工具的功能。开发工具是 3 个应用编程接口(APIS)，它们分别是管理者服务 API(Manager Services API)、代理服务 API(Agent Services API)和数据库/拓扑图 API(Database/topology Map Services API)。

(6) 具备丰富的用户工具。Sun Net Manager 的用户工具很丰富，这些工具主要有如下几种。

① 管理控制台(Management Console)：控制台是一个中央管理应用，它具有面向用户的图形接口，使管理人员能够启动管理任务并显示管理信息。通过控制台，管理员能够解决许多类型的管理问题，如：设备配置设定、故障报警和诊断、网络资源的监控与控制、系统网络容量规划和管理等。系统启动后，屏幕出现 Sun NetManager Console 窗口。之后便可以利用网络管理软



件，对系统进行监控，达到网络管理的目的。如图 8-5 所示的是 Sun NetManager Console 窗口中的网络拓扑结构图。

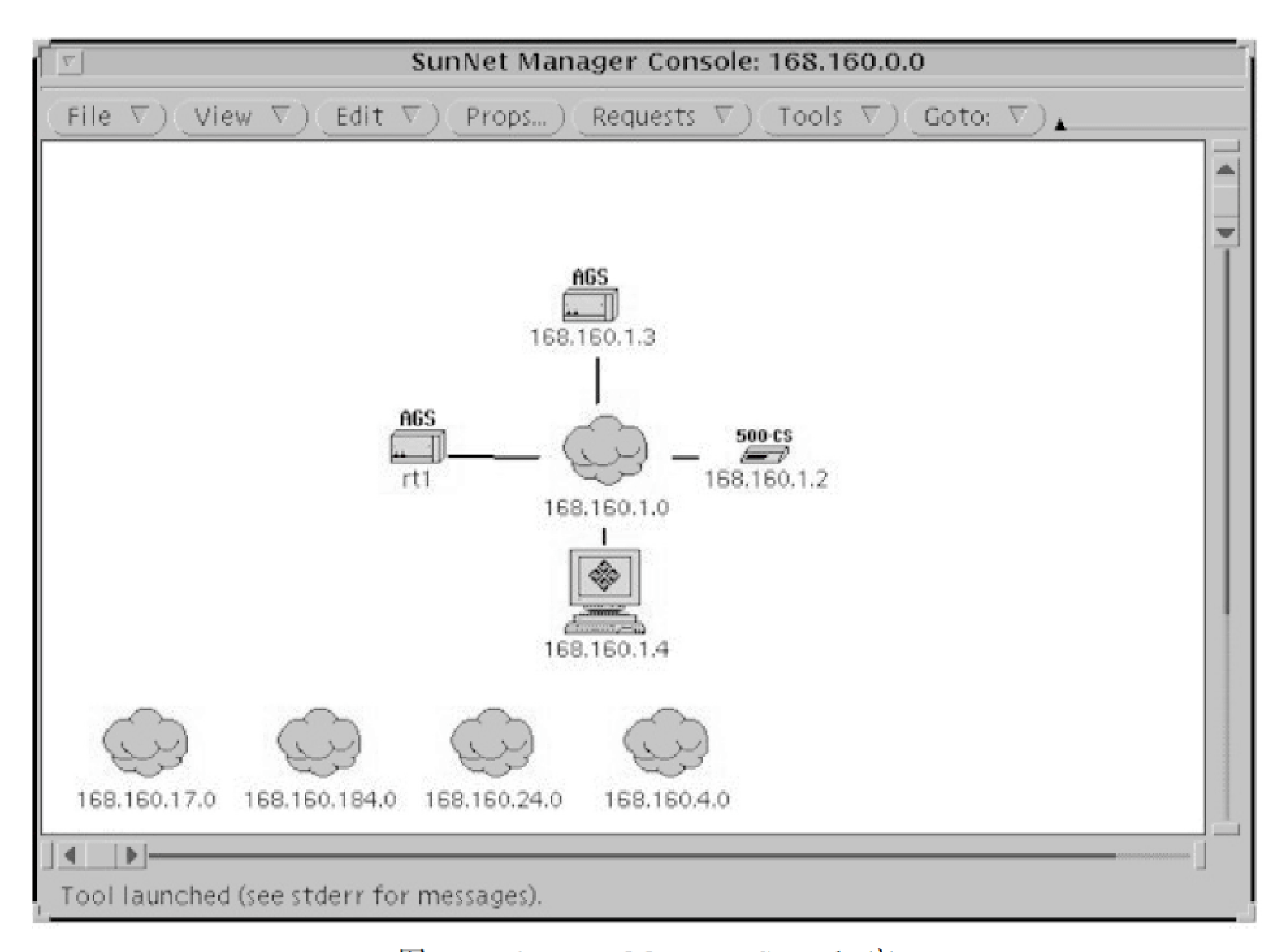


图 8-5　SunNet Manager Console 窗口

② 搜寻工具(Discover Tool)：搜寻工具能够自动发现 IP 和 SNMP 设备，写入管理数据库，并构造网络的图形表示，为建立、显示和配置数据库节省了时间。

③ 版面排列工具(Solstice Domain Manager)：版面排列工具能够从管理数据库中读取信息。并自动将设备和连接按下列 3 种版面排列方式之一显示，这 3 种方式是：层次式、弧形式、对称式。版面排列工具还提供了一个浏览信息窗口，通过这个窗口可以知道目前浏览的是网络的哪个部分。版面排列工具还支持拓扑图的打印。

④ IPX 搜寻工具(IPX Discover)：Sun Net Manager 2.3 能够输入已存在于 Novell Manage Wise 网络管理控制台的拓扑图，因此它能够浏览到 NetWare LAN 的 PC。Sun Net Manager 2.3 能够通过 Novell Management Agent 2.0 管理 NetWare 服务器的文件系统、打印队列、用户组和其他属性。

⑤ 浏览工具(Browser Tool)：浏览工具可用来检索和设置被管设备 MIB 中的 SNMP 属性。管理员还能从特定属性中得到更多信息，包括属性名、属性类型、存取信息和网络地址。

⑥ 图形工具：图形工具通过多维的、可比较的图形来表示动态的或日志化的网络信息。例如，使用图形来显示服务器的 CPU 利用率、负载峰值等信息。这些有利于鉴别统计趋势，诊断潜在的网络问题或瓶颈。

8.4 基于 Windows 的网络管理

8.4.1 SNMP 服务

随着 SNMP 在网络管理上的广泛应用，以及 Windows 操作系统的广泛流行，Windows 已经成为 SNMP 应用和开发的一个重要平台。为此，了解和掌握 SNMP 在 Windows 中的配置和应用非常必要。

首先看一下 SNMP 在 Windows 平台中的应用。SNMP 是 TCP/IP 协议组的一部分，最早被开发出来是为了监视路由器和网桥，并对它们进行故障排除。SNMP 提供了在如下系统之间监视并交流状态信息的能力：运行 Windows NT 内核的计算机、小型或大型计算机；LAN Manager 服务器；路由器、网桥或有源集线器；终端服务器。

基于 Windows 的 SNMP 使用由管理系统和代理组成的分布式体系结构，如图 8-6 所示。有了 SNMP 服务，基于 Windows 的计算机就可以向 TCP/IP 网络上的 SNMP 管理系统报告其状态。当主机请求状态信息或发生重大事件（例如当主机的硬盘空间不足）时，SNMP 服务就会把状态信息发送到一个或多个主机上。

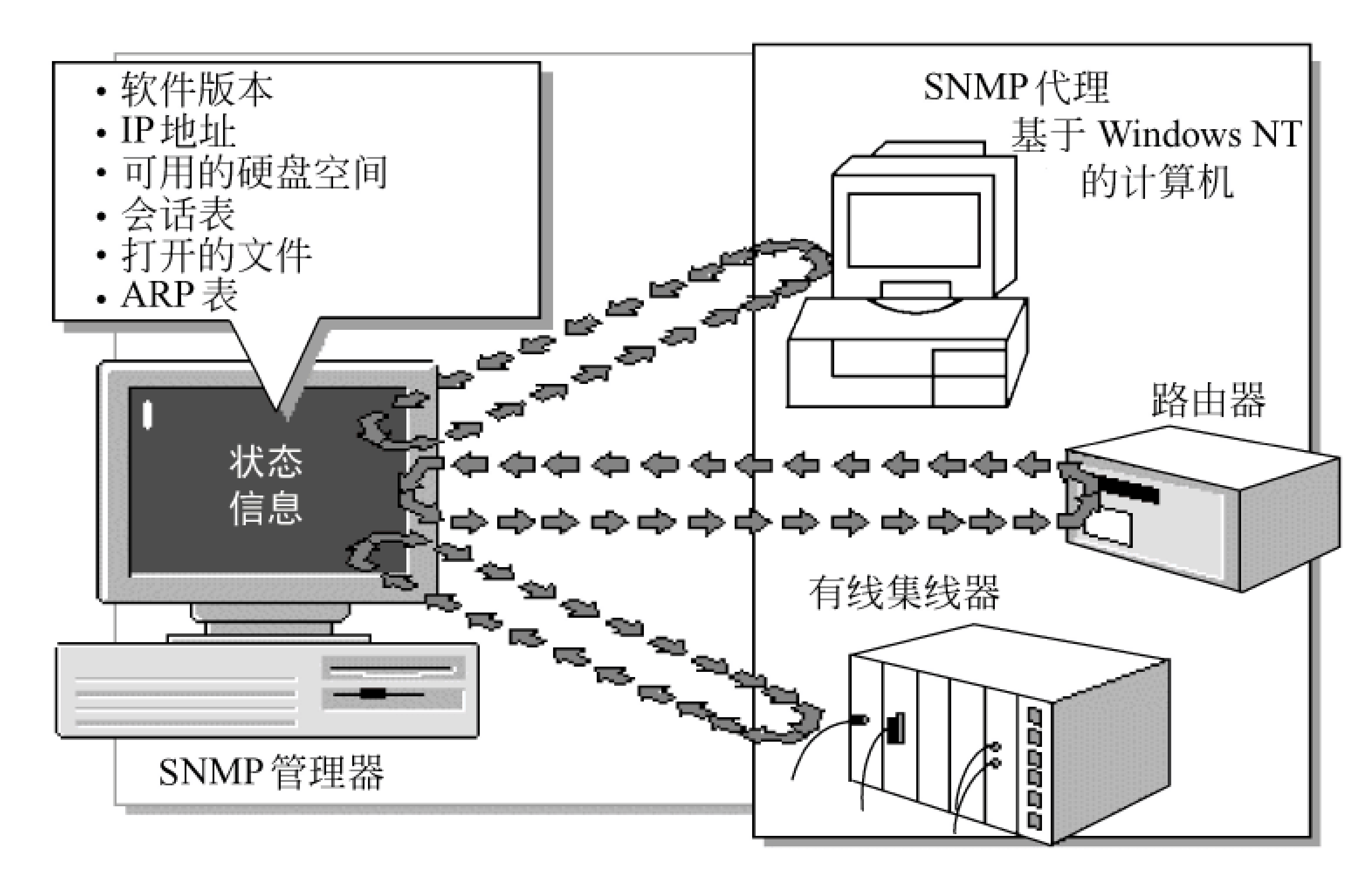


图 8-6　管理和代理组成的分布式结构

Windows 是 SNMP 理想的开发平台。Windows 支持 TCP/IP 网络和图形用户接口，利用这

些特性开发 SNMP 管理系统和代理软件非常方便。Windows 也支持并发的系统服务。一个 Win32 系统服务可以在后台运行，它的开始和停止无需系统重启动。SNMP 就是运行于 Windows 之上的一个系统服务软件。

所谓服务是一种特殊的 Win32 应用软件，它通过 Win32 API 与 Windows 的服务控制管理器接口，一般在后台运行。它的作用是监视硬件设备和其他系统进程，提供访问外围设备和操作系统辅助功能的能力。系统服务在系统启动时或用户登录时自动开始运行。

Microsoft SNMP 服务向运行 SNMP 管理软件的任何 TCP/IP 主机提供 SNMP 代理服务。SNMP 服务包括：处理多个主机对状态信息的请求；当发生重要事件（陷阱）时，向多个主机报告这些事件；使用主机名和 IP 地址来标识向其报告信息和接收其请求的主机；启用计数器监视 TCP/IP 性能。图 8-7 给出了 SNMP 服务体系结构模型。

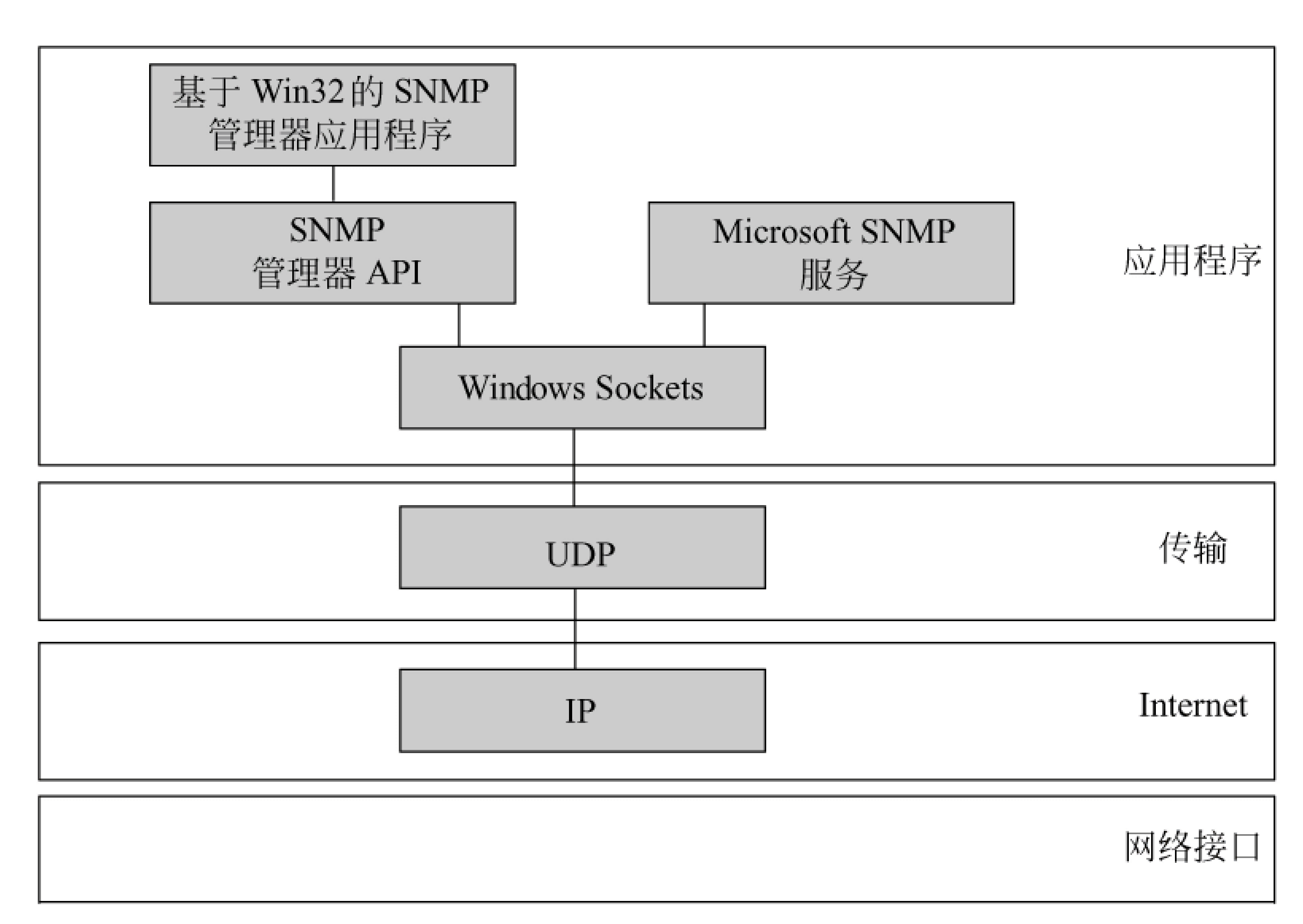


图 8-7　SNMP 服务体系模型

写入到 Windows Sockets API。这允许将管理系统的调用写入到 Windows Sockets。通过用户数据报协议（UDP 端口 161）发送并接收消息，并使用 IP 支持对 SNMP 消息的路由。提供扩展代理动态链接库（DLL），来支持其他 MIB。第三方可以开发他们自己的 MIB，与 Microsoft SNMP 服务一起使用。包括 Microsoft Win32® SNMP 管理器 API，以便简化 SNMP 应用程序的开发。

Windows 的 SNMP 服务包括两个应用程序。一个是 SNMP 代理服务程序 SNMP. EXE，另一个是 SNMP 陷入服务程序 SNMPTRAP. EXE。SNMP. EXE 接收 SNMP 请求报文，根据要求发送响应报文，能对 SNMP 报文进行语法分析，对 ASN. 1 和 BER 编码/译码，也能发送陷入报

文，并处理与 WinSock API 的接口，Windows 98 也含有这个文件。SNMPTRAP. EXE 监听发送给 Windows NT 主机的陷入报文，然后把其中的数据传送给 SNMP 管理 API，Windows 98 没有该陷入服务文件。

Windows 的 SNMP 代理服务是可扩展的，即允许动态地加入或减少 MIB 信息。这意味着程序员不必修改和重新编译代理程序，只须加入或删除一个能处理指定信息的子代理就可以了。Microsoft 把这种子代理叫做扩展代理，它处理私有的 MIB 对象和特定的陷入条件。当 SNMP 代理服务接收到一个请求报文时，它就把变量绑定表的有关内容送给对应的扩展代理。扩展代理根据 SNMP 的规则对其私有的变量进行处理，形成响应信息。SNMP 代理服务和扩展代理以及陷入服务与 Win32 操作系统的关系如图 8-8 所示。

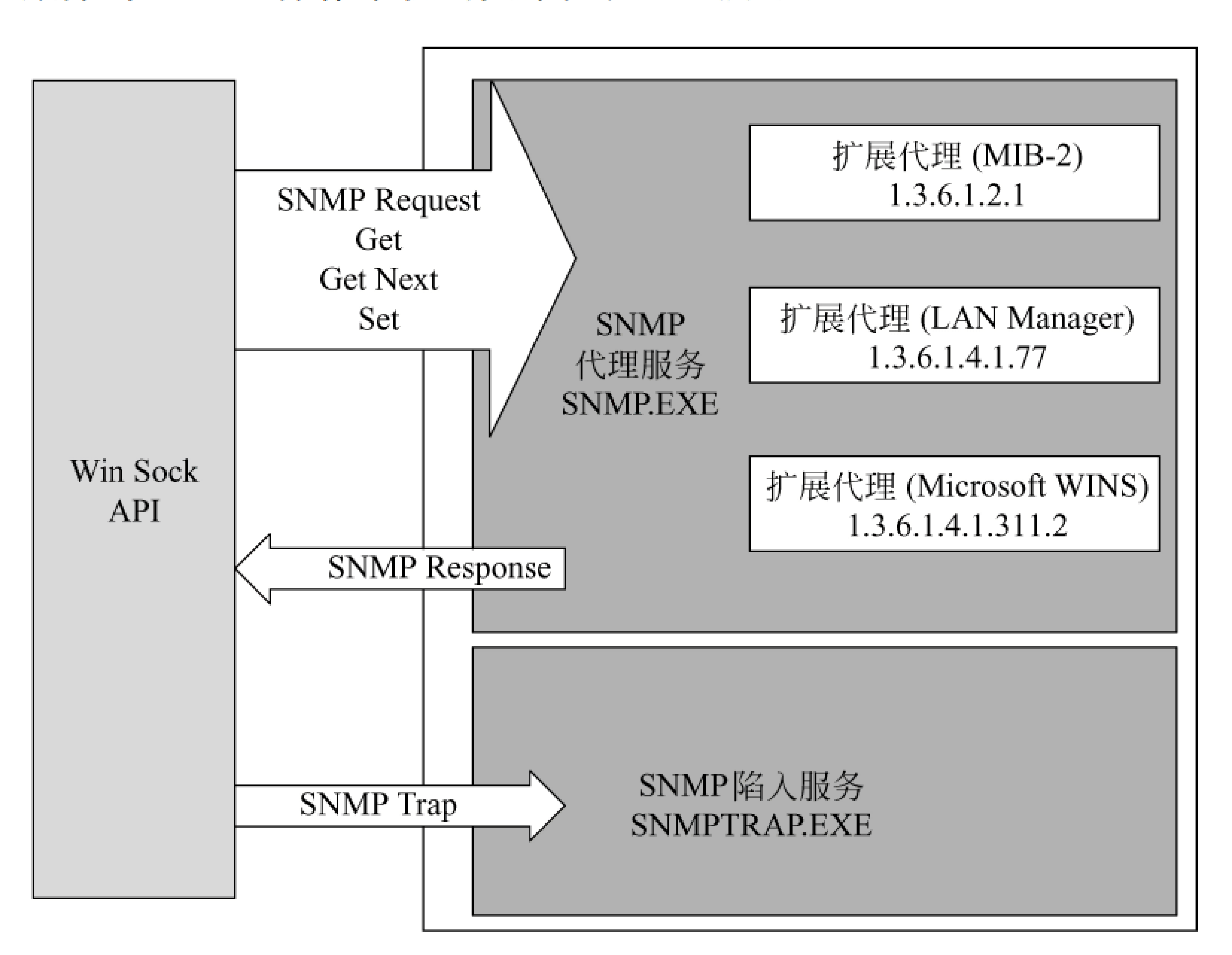


图 8-8　SNMP 服务和扩展代理

SNMP API 是 Microsoft 为 SNMP 协议开发的应用程序接口，是一组用于构造 SNMP 服务、扩展代理和 SNMP 管理系统的库函数。

SNMP 陷入服务监视从 WinSocket API 传来的陷入报文，然后把陷入数据通过命名管道传送给 SNMP 管理 API。管理 API 是 Microsoft 为开发 SNMP 管理应用提供的动态链接库，是 SNMP API 的一部分。管理应用程序从管理 API 接收数据，向管理 API 发送管理信息，并通过管理 API 与 WinSocket 通信，实现网络管理功能。SNMP 陷入服务和 API 的交互作用如图 8-9 所示。

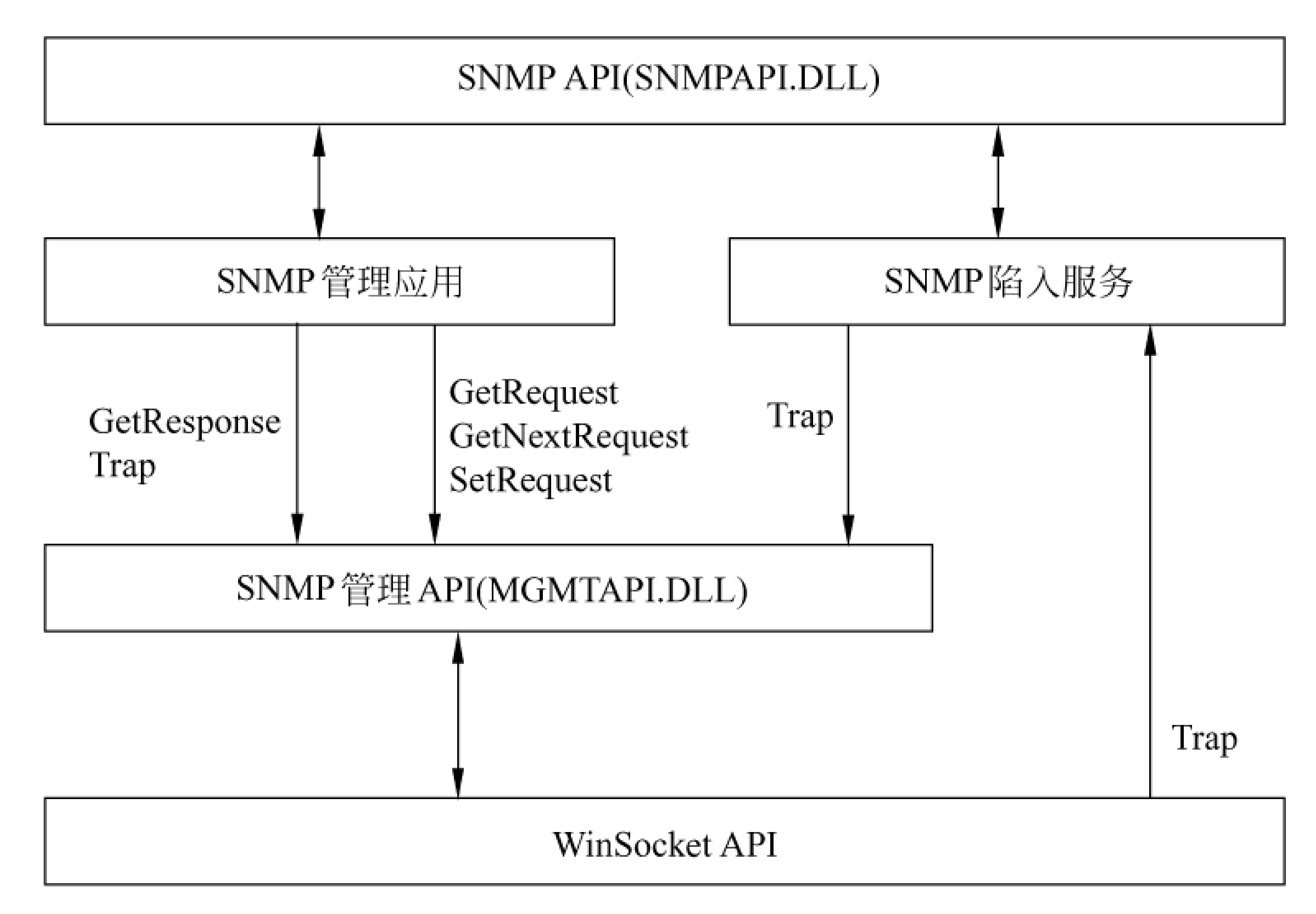


图 8-9　SNMP 陷入服务和 API 的交互作用

8.4.2　SNMP 服务运行

若要确保 SNMP 服务正常运行，需要在以下几个方面做好准备工作：

(1) 主机名和 IP 地址。在安装 SNMP 服务之前，对于要向其发送 SNMP 陷阱或系统中响应 SNMP 请求的主机，要确保拥有其主机名或 IP 地址。

(2) 主机名解析。SNMP 服务使用一般的 Windows 主机名解析方法，将主机名解析为 IP 地址。如果使用主机名，一定要确保将所有相关计算机的主机名到 IP 地址的映射添加到相应的解析源(如 Hosts 文件、DNS、WINS 或 Lmhosts 文件)中。

(3) 管理系统。管理系统是运行 TCP/IP 协议和第三方 SNMP 管理器软件的所有计算机。管理系统向代理请求信息。要使用 Microsoft SNMP 服务，需要至少一个管理系统。

(4) 代理。SNMP 代理向管理系统提供所请求的状态信息，并报告特别事件，是一台运行 Microsoft SNMP 服务的、基于 Windows 的计算机。

(5) 定义 SNMP 团体。团体是运行 SNMP 服务的主机所属的小组。团体由团体名识别。对于接收请求并启动陷阱的代理以及启动请求并接收陷阱的管理系统，使用团体名可为它们提供基本的安全和环境检查功能。代理不接受所配置团体以外的管理系统的请求。

考虑到要与多个团体的 SNMP 管理器进行通信，SNMP 代理可以同时是多个团体的成员。如图 8-10 所示，有两个已定义的团体：Public 和 Public2。

只有作为同一团体成员的代理和管理器才能相互通信。例如：Agent1 可以接收 Manager2

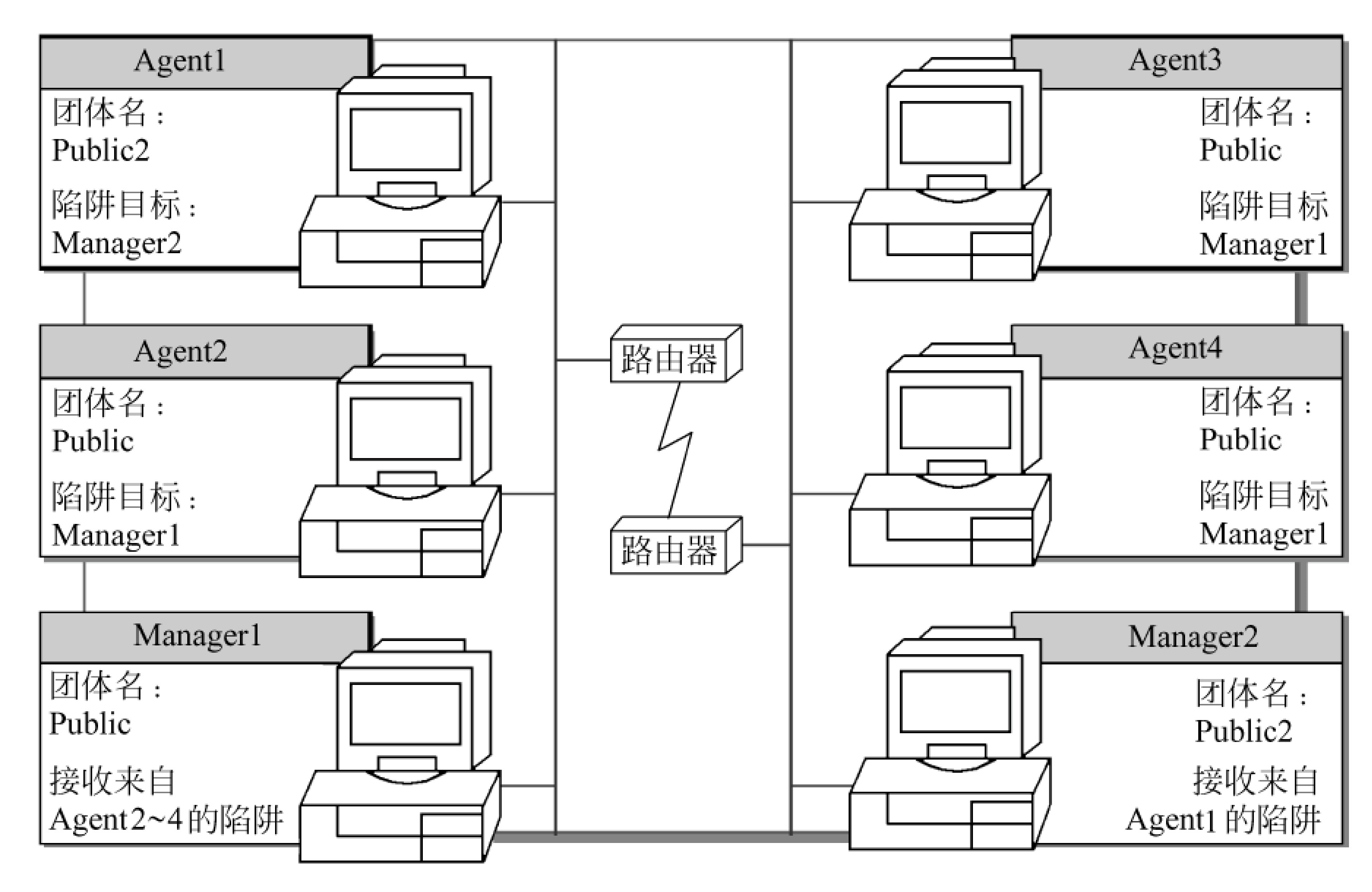


图 8-10　定义团体

的消息并向它发送消息，因为它们都是 Public2 团体的成员；Agent2～4 可以接收 Manager1 的消息，并向它发送消息，因为它们都是默认团体 Public 的成员。SNMP 服务的工作过程如图 8-11 所示。

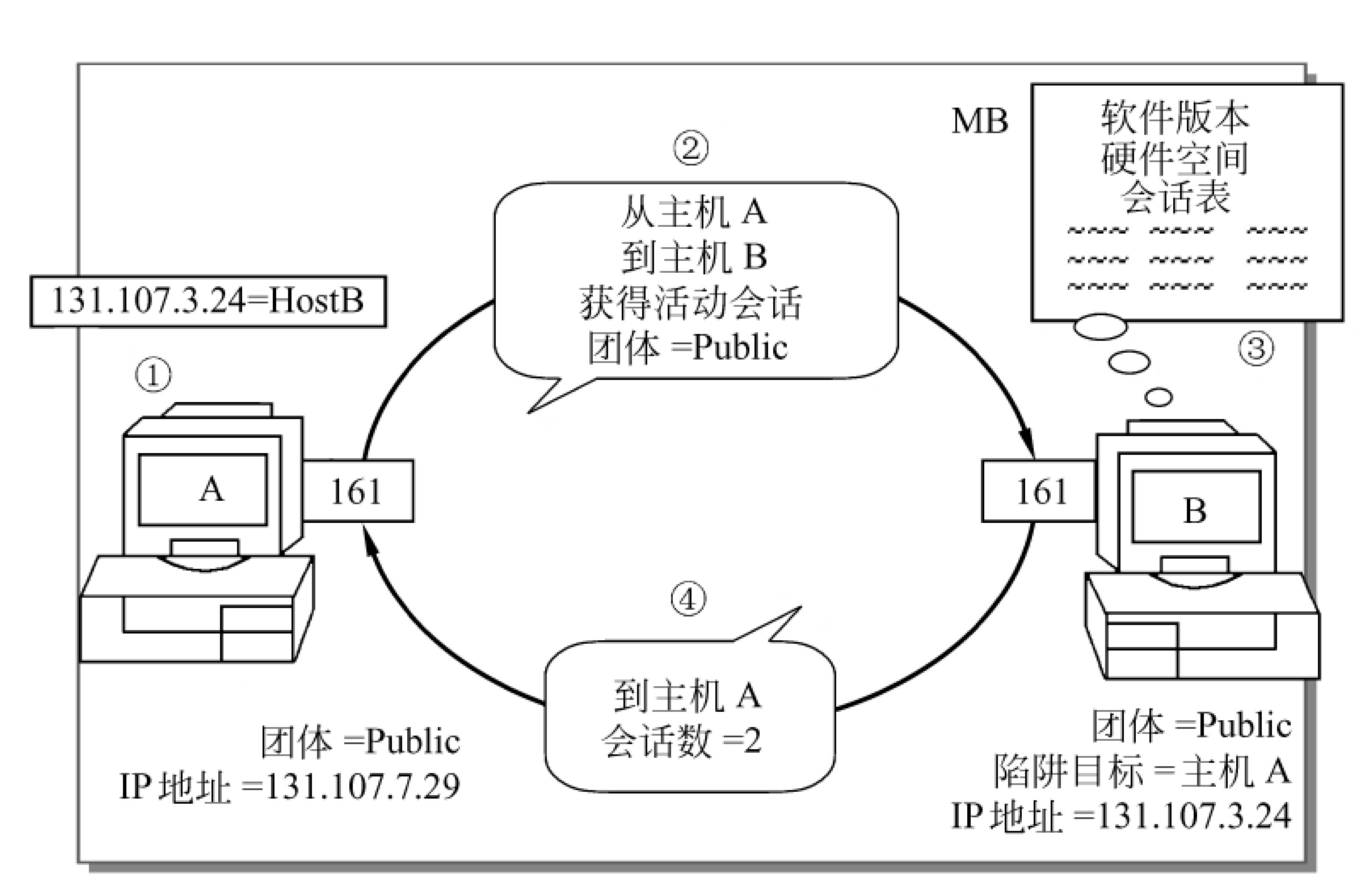
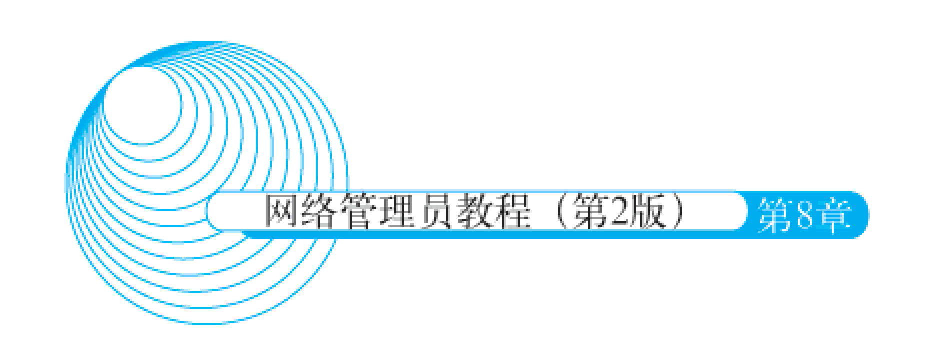


图 8-11　SNMP 服务工作过程



下面的步骤概括了 SNMP 服务如何对管理系统的请求作出响应：

(1) SNMP 管理系统使用一个代理的主机名或 IP 地址，将请求发送给该代理。该应用程序将请求传递给套接字(UDP 端口)161。使用任何可用的解析方法，包括 Hosts 文件、DNS、WINS、B 节点广播或 Lmhosts 文件，将主机名解析为 IP 地址。

(2) 建立包含如下信息的 SNMP 数据包：针对一个或多个对象的 get、get-next 或 set 请求；团体名和其他验证信息；数据包被路由到代理上的套接字(UDP 端口)161。

(3) SNMP 代理在其缓冲区中接收该数据包。对团体名进行验证，如果团体名无效或数据包格式不正确，则将它丢弃。如果团体名有效，代理将验证源主机名或 IP 地址。需要说明的是，必须对代理进行身份验证，才能接收来自管理系统的数据包，否则丢弃数据包。然后将请求传递到相应的 DLL。再将对象标识符映射到相应的 API 函数，然后调用此 API，DLL 将把信息返回给代理。

(4) SNMP 数据包与所请求的信息一起被返回给 SNMP 管理器。

8.4.3 SNMP 服务的安装与配置

SNMP 服务的安装方法同其他服务的安装方法类似，但是需要注意的是安装 SNMP 服务首先必须安装 TCP/IP 协议。

以 Windows 2000 下 SNMP 服务的安装与配置为例，具体操作步骤如下。

1) 安装 SNMP 服务

(1) 以管理员身份登录，在“控制面板”中选择“网络和拨号连接”并双击它，系统弹出网络和拨号连接窗口，选择菜单“高级”菜单下的“可选网络组件”，如图 8-12 所示。



图 8-12　添加网络组件

(2) 系统弹出“可选网络组件向导”窗口，在“可选网络组件向导”窗口中的组件列表中选择“管理和监视工具”，单击“下一步”按钮。如图 8-13 所示。

(3) 系统提示插入系统安装光盘，将相应的光盘放入 CD-ROM 后，单击“确定”按钮，如图 8-14 所示。

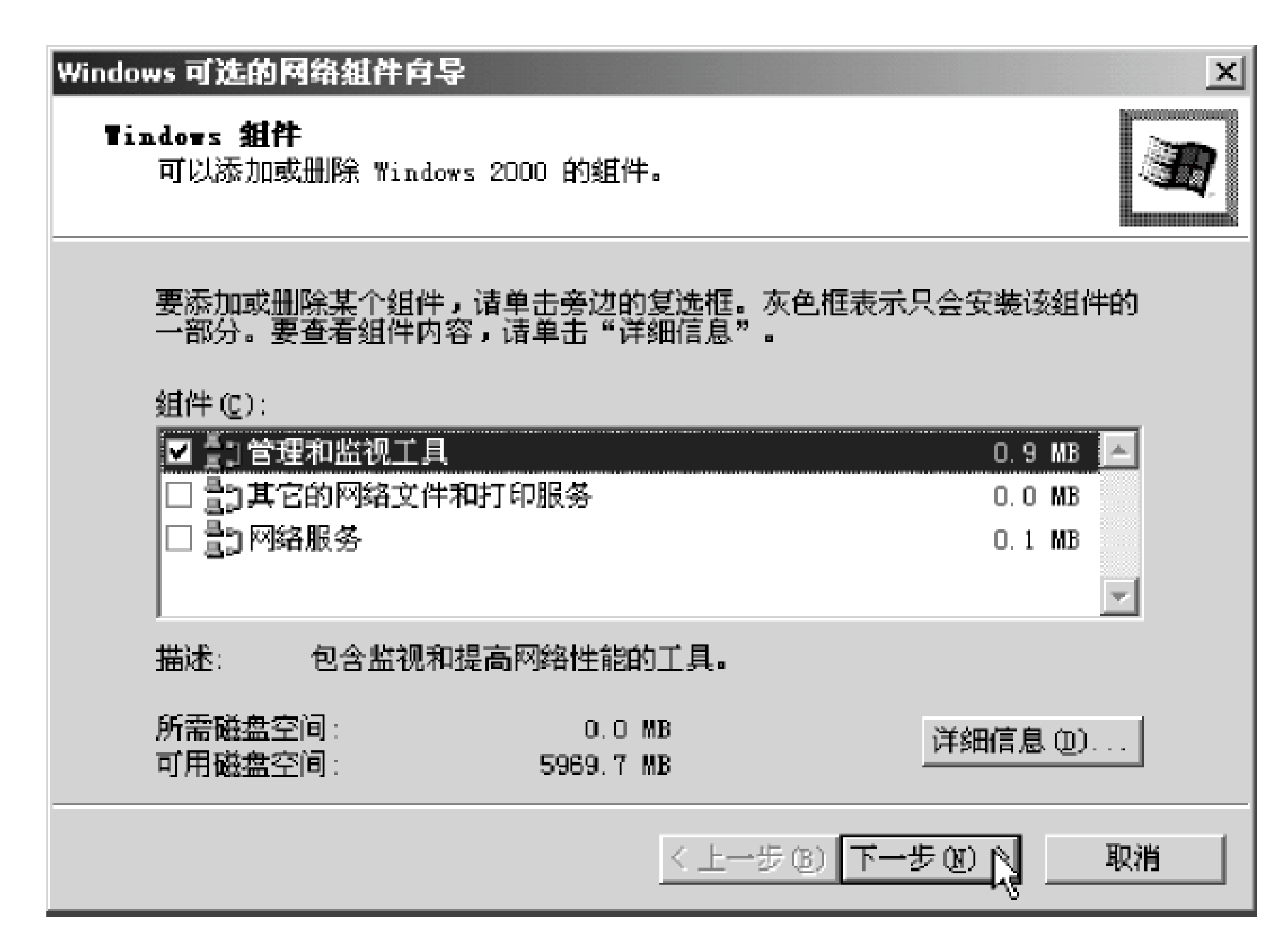


图 8-13　可选网络组件向导



图 8-14　插入系统安装光盘

（4）系统自动从安装光盘中添加 SNMP 服务，并完成 SNMP 服务的安装，如图 8-15 所示。

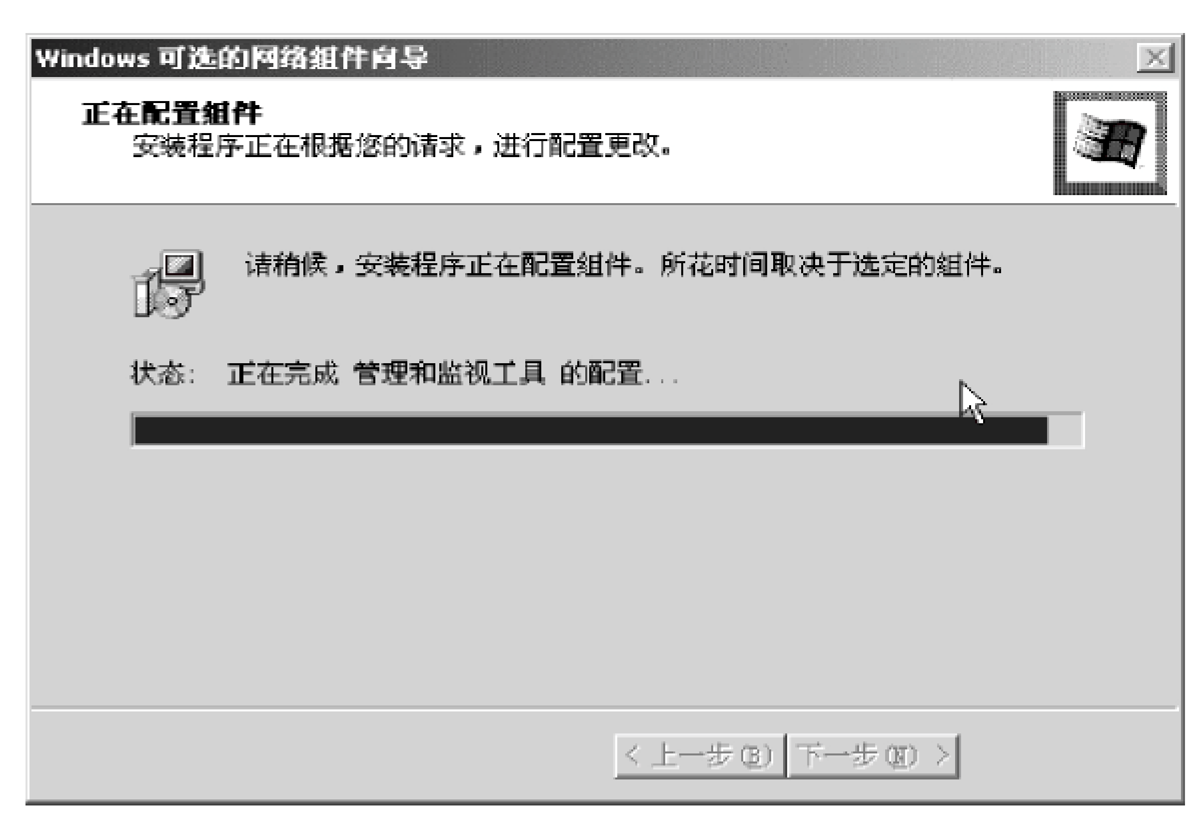
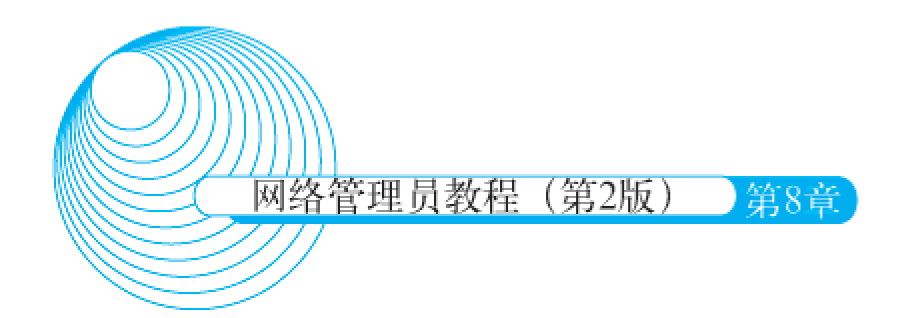


图 8-15　添加 SNMP 服务



2）配置 SNMP 服务

（1）在“控制面板”中双击“管理工具”选项，弹出管理工具窗口，如图 8-16 所示。



图 8-16　选择服务

（2）在管理工具窗口中双击“服务”选项，弹出如图 8-17 所示的服务窗口。

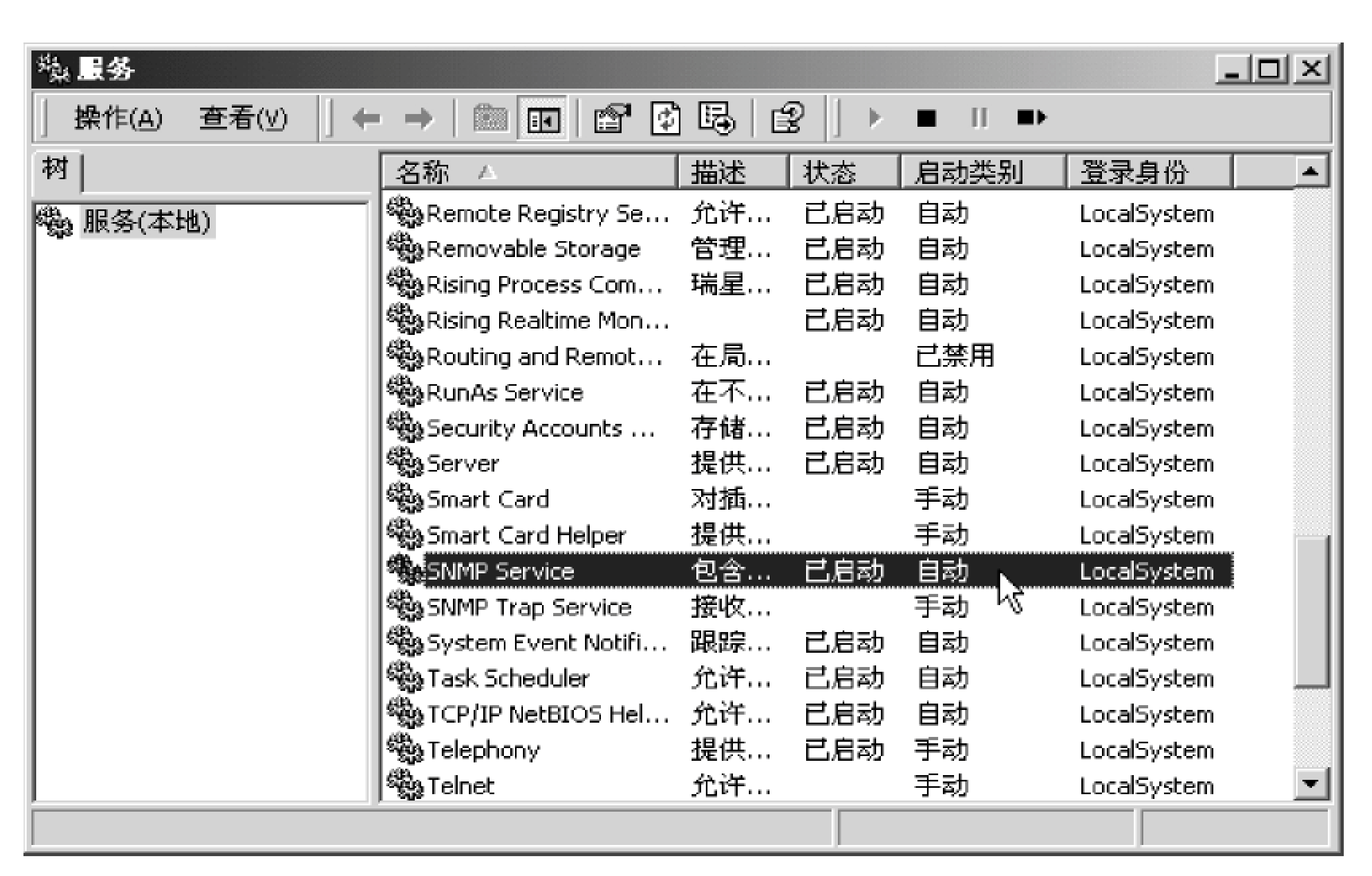


图 8-17　选择 SNMP 服务

（3）在服务窗口中选择 SNMP Service，并双击它，弹出“SNMP 服务属性”窗口，如图 8-18 所示。SNMP 服务使用的主要信息都在这个窗口中进行配置。

（4）选择“代理”选项进行代理配置，如图 8-19 所示。其中的联系人、位置和服务分别对应系统组中的 3 个对象 sysContact、sysLocation 和 sysServices。



图 8-18　SNMP 属性设置

图 8-19　代理设置

（5）选择“陷阱”选项进行陷阱配置，如图 8-20 所示。需要配置的内容包括团体名和陷阱目标。其中团体名的输入要注意大小写，陷阱目标可以是 IP/IPX 地址或 DNS 主机名。

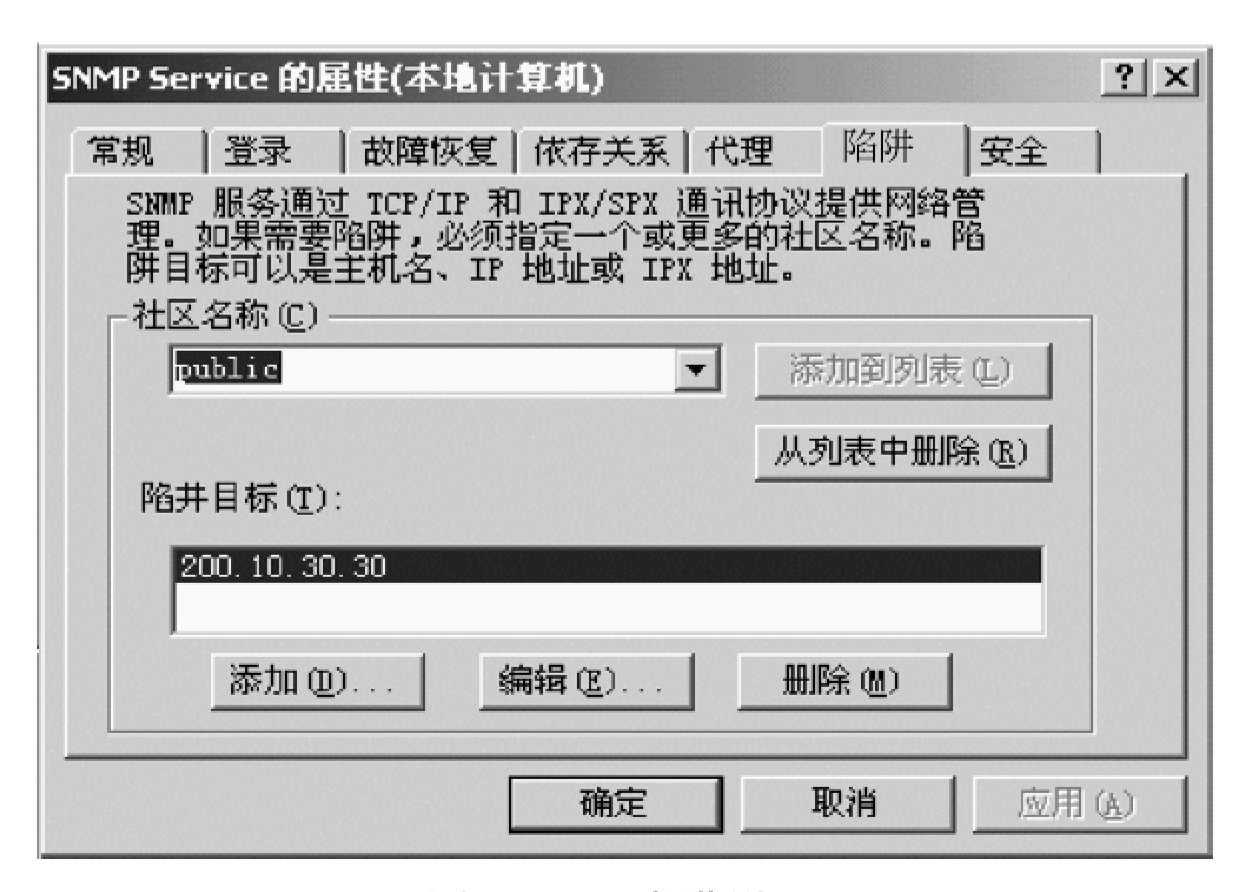


图 8-20　陷阱设置

（6）选择“安全”选项进行安全配置，如图 8-21 所示。该部分内容是为发送需要认证的陷入报文而设置的。如果不选择“发送身份认证陷阱”选项，则任何团体名都是有效的。另外可以配置代理接受任何主机或只接受特定主机的 SNMP 包，可以在该选项中进行设置。



图 8-21　安全设置

(7) 上述内容设置完毕后，单击“确定”按钮，退出 SNMP 属性配置窗口，新的配置就起作用了。

8.4.4　SNMP 服务的测试

在 SNMP 服务安装、配置完成后重新启动系统，SNMP 服务就开始工作，工作站就可以接受 SNMP 的询问了。假设一台 Windows NT 安装了 MIB-2 扩展代理和 LAN Manager 扩展代理，另外一台 Windows 98 也安装了 MIB-2 扩展代理，现在就可以向 SNMP 代理发出询问，并检查它的响应了。那么如何对 SNMP 服务进行测试呢？

Microsoft 提供了一个实用程序 SNMPUTIL，可以用于测试 SNMP 服务，也可以测试用户开发的扩展代理。

需要说明的是：SNMPUTIL 是用 Microsoft 的管理 API(MGMTAPI.DLL)写的，由于在 Windows 98 中没有管理 API，所以在 Windows 98 下不能运行。SNMPUTIL 是一个 MS-DOS 程序，需要在 DOS 命令窗口中运行。SNMPUTIL 的用法是：

usage：snmputil[get|getnext|walk]agentaddress community oid[oid…]snmputil trap

可以使用 SNMPUTIL 发送 GetRequest 或 GetNextRequest 报文，也可以用 SNMPUTIL 遍历整个 MIB 子树。一种较好的测试方法是同时打开两个 DOS 窗口，在一个窗口中用 SNMPUTIL 发送请求，在另一个窗口中用 SNMPUTIL 接收陷入。

注意：SNMPUTIL 没有包含 set 命令，这是简化了的实现。

下面是使用 SNMPUTIL 测试 SNMP 服务的例子，假设代理的 IP 地址是 200.10.30.123，有效的团体名是 public，则可以完成以下测试。

（1）用 GetRequest 查询变量 sysDesc（可省去 MIB-2 的标识符前缀 1.3.6.1.2.1）。

```
snmputil get 200.10.30.123 public 1.1.0
```

（2）用 GetNextRequest 查询变量 sysDesc。

```
snmputil get 200.10.30.123 public 1.1
```

（3）用 GetNextRequest 查询一个非 MIB-2 变量（.1.3.6.1.4.1.77.1.3 中的第一个“.”是必要的，否则程序就找到 MIB-2 中去了）。

```
snmputil getnext 200.10.30.123 public.1.3.6.1.4.1.77.1.3
```

（4）用 walk 遍历 MIB-2 系统组变量。

```
snmputil walk 200.10.30.123 public1
```

（5）用 walk 遍历整个 MIB-2 子树（可以接收到扩展代理 INETMIB.DLL 支持的所有变量的值）。

```
snmputil walk 200.10.30.123 public.1.3.6.12.1
```

（6）测试 SNMP 陷入服务。

首先在上述第二个窗口中启动 SNMPUTIL，监听陷入 snmputil trap，然后在另一个窗口中发送请求，使用一个无效的团体名。

```
snmputil getnext 200.10.30.123 test 1.1
```

由于没有团体名 test，所以团体名认证出错，陷入窗口中将出现一个认证陷入：

```
smnputil: trap generic=4 specific=0 from—>200.10.30.123
```

测试的示例如图 8-22 所示。

（7）测试冷启动陷入。保持第二个窗口继续监听陷入，然后先停止 SNMP 服务，再重启动 SNMP 服务，在陷入窗口中将会收到由扩展代理发出的冷启动陷入：

```
smnputil: trap generic=1 specific=0 from—>200.10.30.123
```

上述 SNMPUTIL 实用程序在 Visual C++ 安装盘中附带，用户使用时需要进行编译。另外在 Windows 2000/XP 的安装盘中附带了一个图形界面的测试程序 SNMPUTILG.EXE，用户可以安装这个测试工具。SNMPUTILG 的安装路径为 support/tools/setup.exe。

```
命令提示符 - snmputil trap
I:\SNMPUTIL>snmputil trap
snmputil: listening for traps...
snmputil: trap generic=4 specific=0
  from -> 200.10.30.123
snmputil: trap generic=4 specific=0
  from -> 200.10.30.123
snmputil: trap generic=4 specific=0
  from -> 200.10.30.123
snmputil: trap generic=0 specific=0
  from -> 200.10.30.123
snmputil: trap generic=0 specific=0
  from -> 200.10.30.123
snmputil: trap generic=0 specific=0
  from -> 200.10.30.123
```

图 8-22 测试 SNMP 陷入服务

当完成安装后，启动方法如图 8-23 所示。程序启动后，出现如图 8-24 所示的界面，其使用方法同 SNMPUTIL，只不过其为图形化的界面而已。

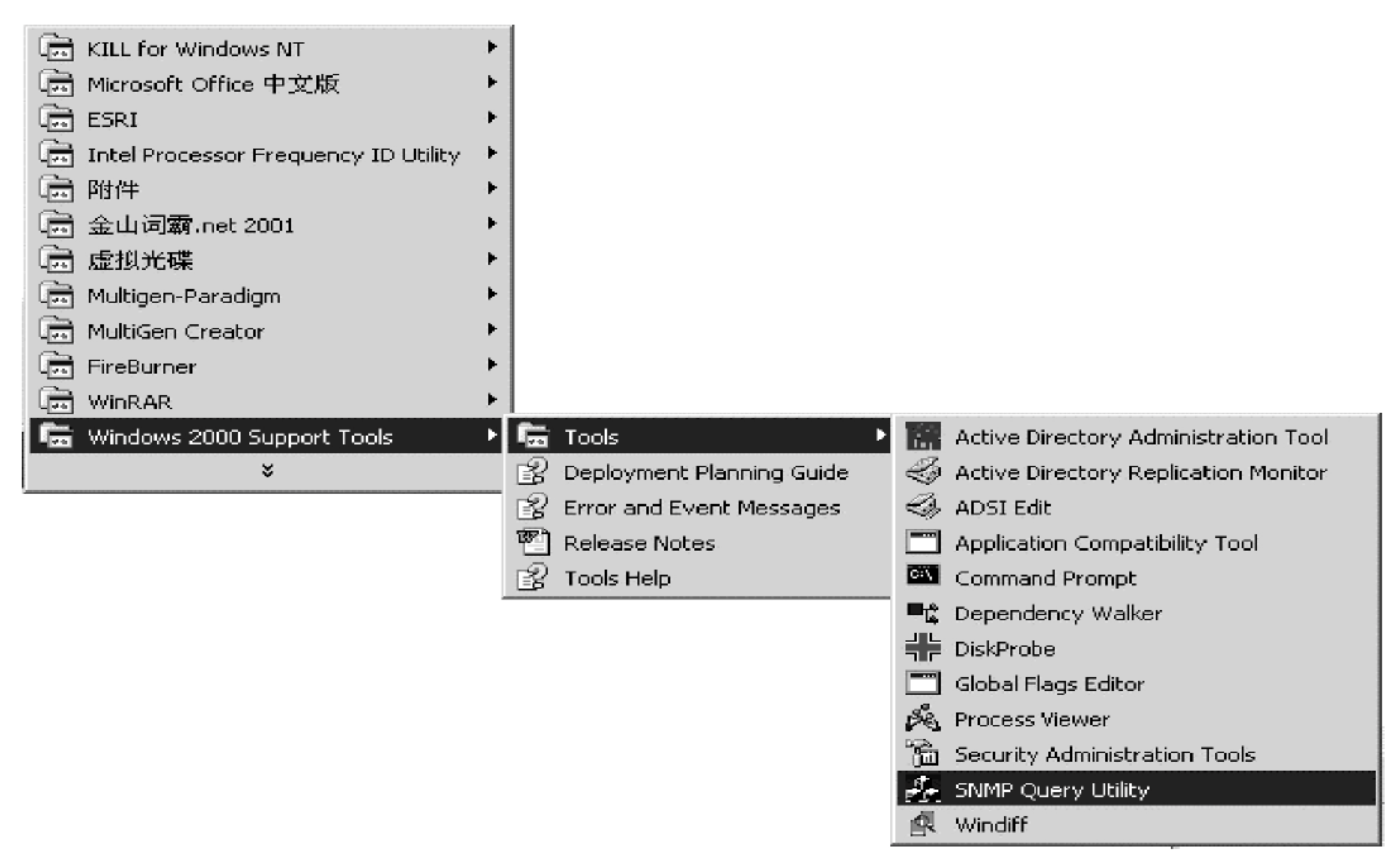


图 8-23 启动 SNMPUTILG 程序

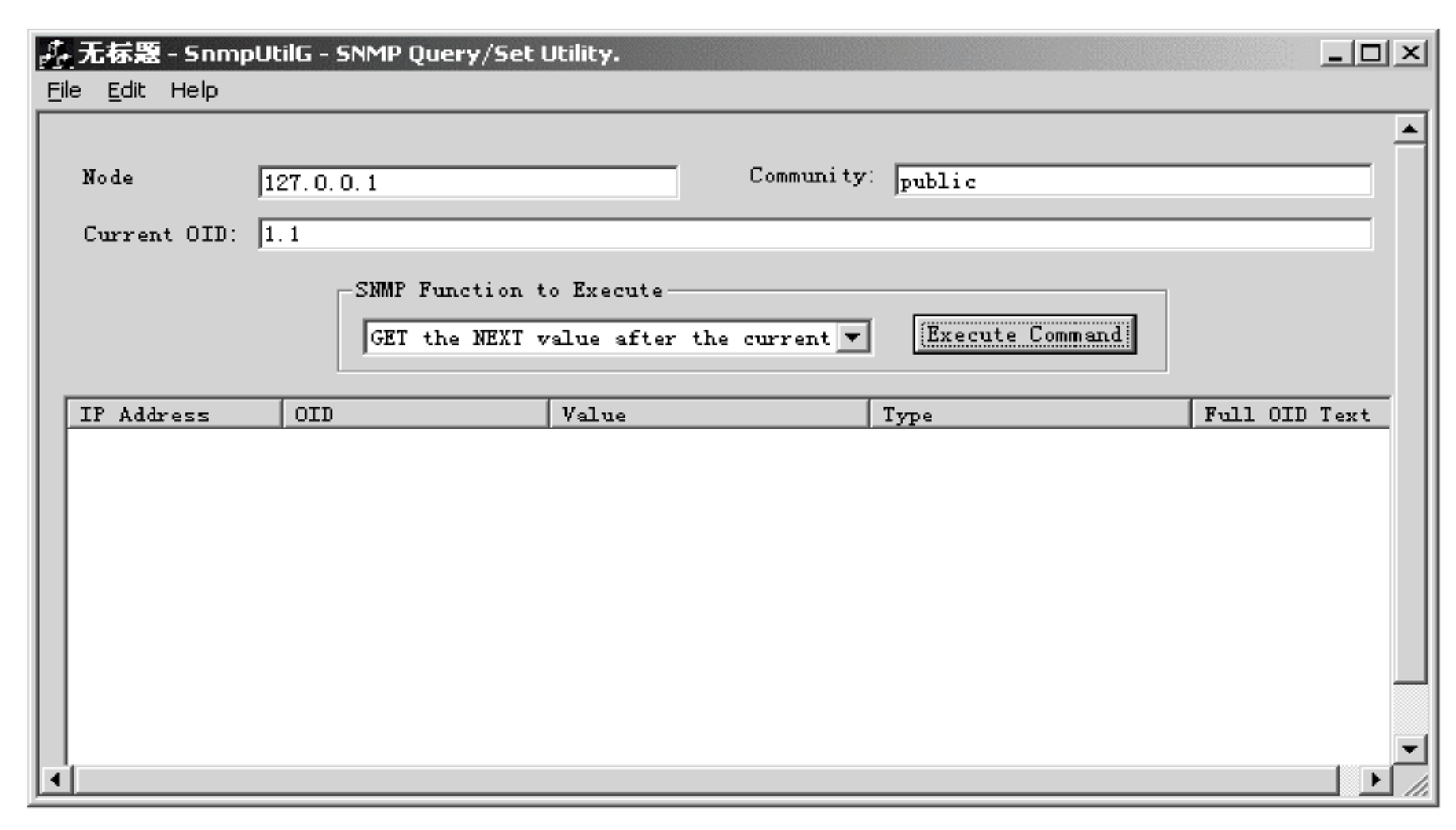


图 8-24 SNMPUTILG 程序界面

8.5 综合企业管理平台 Unicenter TNG

8.5.1 Unicenter TNG 简介

CA 公司的 Unicenter TNG 是一个 Windows 环境的企业系统管理软件。Unicenter TNG 通过面向对象的技术、友好的管理界面、可扩充的体系结构提供了强大的集成管理。它能够提供一个统一简单、稳定可靠的网络管理平台，能够保证系统每周 7 天、每天 24 小时的全天候正常运行及网络资源的有效利用。

Unicenter TNG 作为一种集成化的企业管理解决方案，能够对分布式计算环境中的各种异构网络、系统、应用和数据库平台实施端到端的全面综合管理，不但适用于传统及现代分布式计算环境，同样也适用于因特网和内联网应用环境。

Unicenter TNG 通过使用代理(Agent)获得网络某段内资源信息来分担管理工作，从而实施管理策略和将网络轮询工作局部化，这样可使资源管理尽可能地离开企业网络主干线，而局限在特定的区域里。Unicenter TNG 将整个企业的 IT 资源管理按照企业内的特定业务划分开来，系统管理员只须管理影响每一业务处理的那些相关资源。这种管理角度和模式的转变大大减小了系统及网络管理的复杂性，同时，这种新的管理方法不但可以监控系统资源，还可以查看这些资源间的相互关系。

简单地讲，Unicenter TNG 主要有以下几个特点。

（1）集中管理。Unicenter TNG 给用户提供了一个集中的管理方法，用户通过一台中心管理机，就可以看到所有管理的资源，包括这些管理对象的实时运行情况。即使这些对象的具体物理位置远隔千里，也可以通过端到端的管理模式进行管理。这种端到端的管理模式允许将任何系统或服务集成到其管理框架内，无任何限制。

（2）强大的管理功能。Unicenter TNG 本身提供了强大丰富的管理功能，并可结合合作伙伴和客户的解决方案，为管理复杂的异构网络提供了一个全面的解决方案。通过 Unicenter TNG，网络管理员不仅能够发现问题，而且能够对发现的问题指定相应的处理策略进行自动处理。Unicenter TNG 能够管理系统中的所有资源，包括主机系统、连接设备的路由器和集线器、数据库服务器以及系统数据库等，同时，还能实时监控这些资源的运行情况。

（3）强大的安全功能。Unicenter TNG 提供的安全管理手段包括防火墙、病毒检测、用户访问控制和数据备份等各个方面，提供了从网络系统到应用系统的整体安全管理策略，建立了统一的网络用户和网络资源的整体安全控制系统。

（4）开放性和可扩展性。Unicenter TNG 支持多种硬件平台（如 HP、IBM、UNIX 及 S/390 主机等）和操作系统（如 Windows NT、UNIX 和 MVS 等），同时也支持多种工业标准的网络协议（如 SNA、SNMP、TCP/IP、FTP 等）。Unicenter TNG 提供的框架结构，可以方便地和第三家产品集成，做到菜单和事件报警的高度集成。

（5）从任何地方管理一切。Unicenter TNG 还提供了基于 Web 的浏览界面，支持各种 Web 协议，能够从网络系统的任何地方管理系统资源。

（6）易于学习和使用。Unicenter TNG 为用户提供了丰富的图形界面，包括 2D、3D 及 Web 界面，通过这些图形界面，用户可以完成所有的管理功能，包括：资源事件的浏览、事件的捕获、对事件的动作定义、用户及资产的定义等。另外，全新的三维虚拟现实界面使用户可以更直观地监控和管理分布在网络中的各种资源。

8.5.2 Unicenter TNG 的基本管理功能

Unicenter TNG 提供的基本管理功能适用于管理各种规模的网络，能够使系统简单化、自动化。网络管理员可以根据自身需要来定制系统管理工作站。通常，Unicenter TNG 具有以下几个基本管理功能。

（1）Event Management（事件管理）。Event Management Console 是一个高级的系统管理工具，用作事件管理的接口。该控制台是 Unicenter TNG Enterprise Management GUI 的一个特殊窗口，能让用户完整地查看网络系统上正在发生的事件处理。Event Management 让用户明确所需响应的事件，指定一个或多个自启动的动作。这意味着一旦用户定义了事件和相关动作，Unicenter TNG 遇到相关事件时系统就会自动执行指定的动作。

（2）Workload Management（工作量管理）。Workload Management 对关键操作进行控制，如

调度作业、监测作业顺序、监控作业的失败、坚持时间要求、将作业与机器相匹配，以便作业在机器上有充足的资源足以有效运行等。Workload Management 可以根据存储在工作量管理数据库中的策略的正确次序，自动在正确的时间来选择、调度和提交作业以及作业集。

（3）Job Tracking（作业跟踪）。系统通过图形用户接口 GUI（Graphical User Interfaces）为用户提供调度活动的实时显示，包括作业状态（Job Status）、作业集状态（Jobset Status）和作业流。另外，GUI 提供了活动作业及作业集状态的当前显示，还显示最近完成的作业和作业集的信息。

（4）Automatic Storage Management（自动存储管理）。Automatic Storage Management 具有与大型机采用的同样强大的跨平台和跨网络的存储管理功能。自动存储管理可以对磁带、软盘、CD-ROM 以及类似的设备进行管理，还可以利用廉价磁盘冗余阵列 RAID（Redundant Array of Inexpensive Disks）进行并行存储。

（5）Security Management（安全管理）。Security Management 功能提供了基于策略的安全工具，在操作系统上提供了进一步的安全保障。具体地讲，Unicenter TNG 实现了如下三个逻辑层次的安全：

① 验证。Unicenter TNG 在操作系统的登录和口令功能上增加了安全策略。比如，规定什么人、多长时间必须修改一次口令。

② 授权。Unicenter TNG 的安全策略会优先于操作系统的安全策略发生作用，而且可以生成用户组并创建组策略。Unicenter TNG 可以控制所有账号，包括 UNIX 的超级用户和 Windows NT 管理员。它也可以限制对网络操作系统的访问。

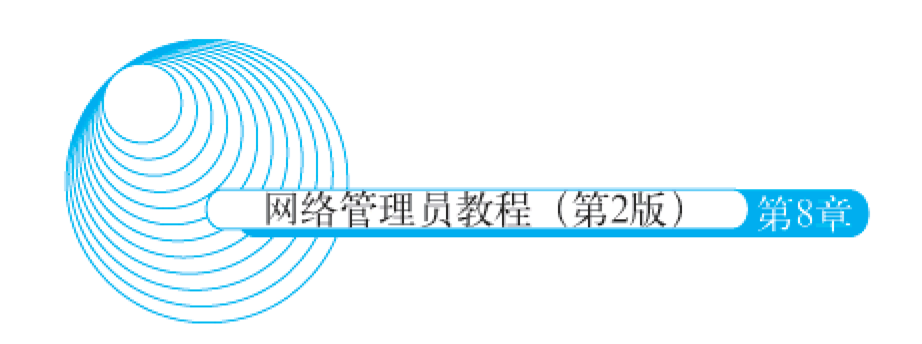
③ 审计跟踪。系统根据用户 ID 或文件访问权限创建审计跟踪。

（6）Problem Management（问题管理）。Problem Management 可以自动进行问题的定义、跟踪和解决。部件定义系统的配置包括硬件、软件、计算机无关设备（如空调和暖气）、无线通信部件、安全系统以及想要跟踪的其他任何部件。问题定义被送入问题管理既可以由管理员手动执行，也可以由机器生成的问题跟踪工具 MGPT（Machine Generated Problem Tracking）自动实现。问题跟踪是基于 Unicenter TNG 事件管理功能监测的活动，可自动开出问题通知单（记录）。

（7）Performance Management（性能管理）。Performance Management 是基于 GUI 的应用软件，将性能和资源使用数据图形化，并进行管理和配置。基本数据是由 Performance Agents 从分布式系统收集而来的。另外，性能管理应用还提供在线实时窗口，显示网络的系统性能。它们还可检查系统长期的历史性能，由此用户可发现性能瓶颈、问题趋势等。

8.5.3 Unicenter TNG Discovery

Unicenter TNG Discovery 能够实现对连网设备的自动检测，而且能用代表网络设备及其关系的对象填充 Unicenter TNG 对象库。对象一旦创建，就可以利用 Unicenter TNG 图形界面进行显示，并通过 Unicenter TNG 企业管理层的应用软件进行监控，比如安全和事件管理器、第三



方管理器应用软件等。

Discovery 能生成一张网络图，但这张图是由 IP 网络的拓扑结构确定的。网络图可以真切地反映网络环境的物理结构，也可以通过 Business Process Views 定制 Unicenter TNG，反映网络环境的逻辑结构，如图 8-25 所示。

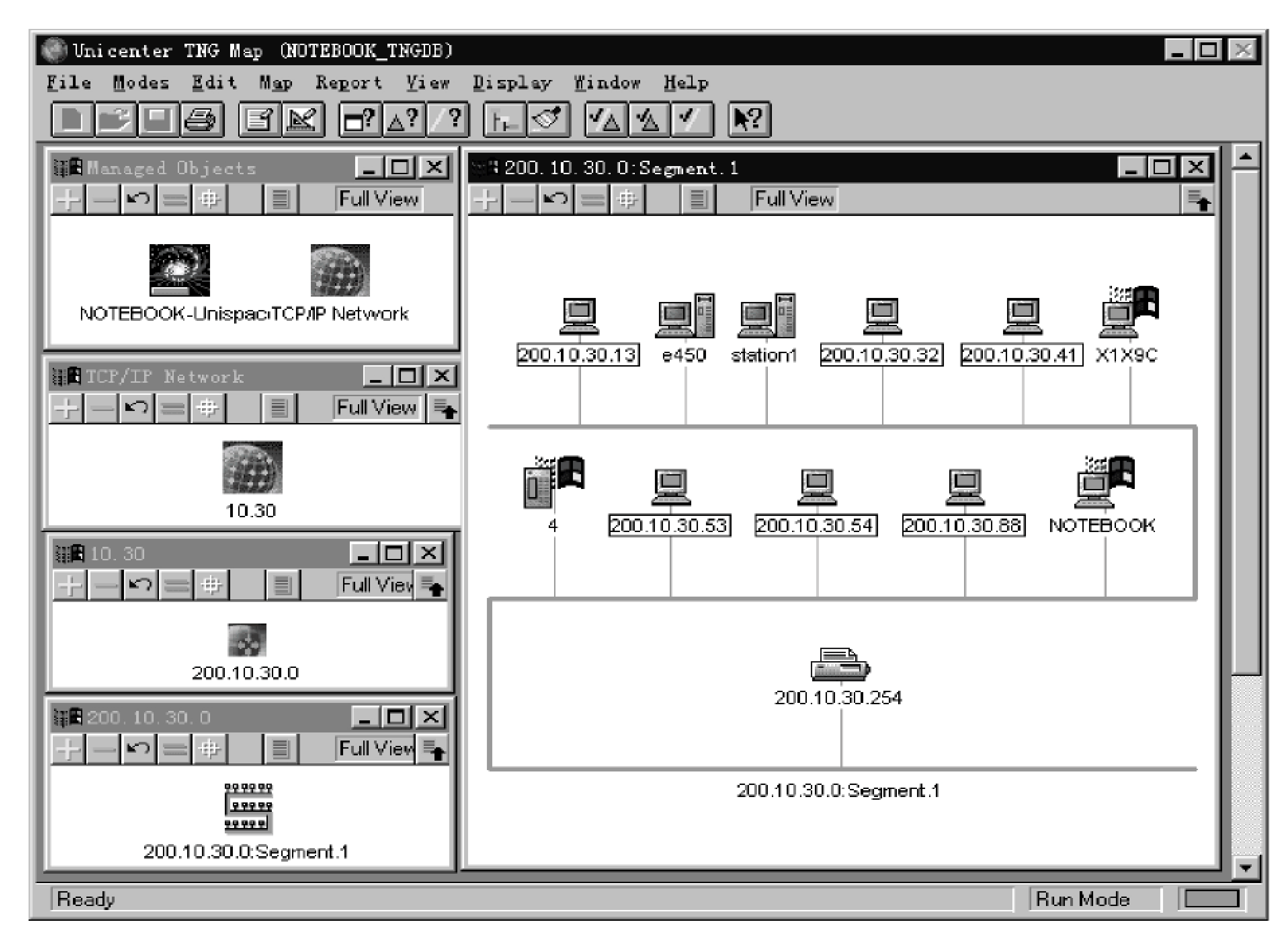


图 8-25　二维图

通常在使用 Unicenter TNG 时都会给生成的网络结构图增加一个背景。这个背景就是网络所处的地理位置。

Unicenter TNG 提供了一些较为常用的背景图形，用户可以进行选择。要增加背景图案，必须处在 Design 模式下，然后在二维窗口顶部的菜单选择 Map，再从 Map 菜单中选择合适的选项。其中包括的选项有大陆(Continents)、国家(Countries)、地区(Regions)、子地区(Sub-Regions)以及组(Groups)。然后拖动对话框上的滚动条，选中所想选择的图形，然后单击 OK 按钮。所选择的背景图案就会在网络结构图下面显示出来，如图 8-26 所示。

通过网络图，可以查看各个网络设备的详细信息，方法是将鼠标移到要查看的网络设备上，单击鼠标右键，从弹出的快捷菜单中选择 Open Details 子菜单，会弹出如图 8-27 所示窗口。在该窗口中，有众多选项可供选择，例如可以查看 SNMP 代理的配置信息，如图 8-28 所示。

另外在网络图中还可以查看网络设备中的 MIB-II 对象的信息，方法是将鼠标移到要查看的

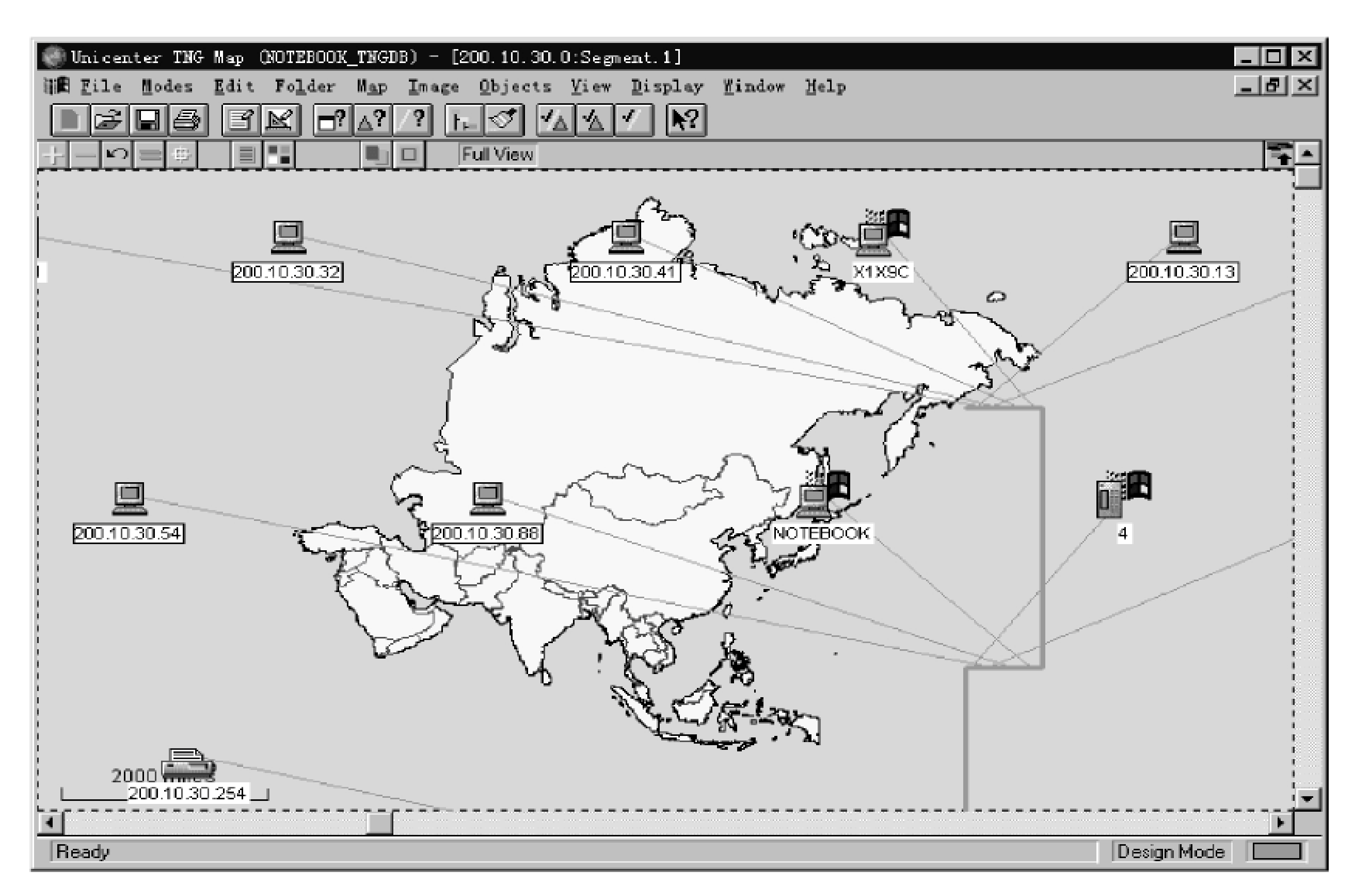


图 8-26　添加背景二维图

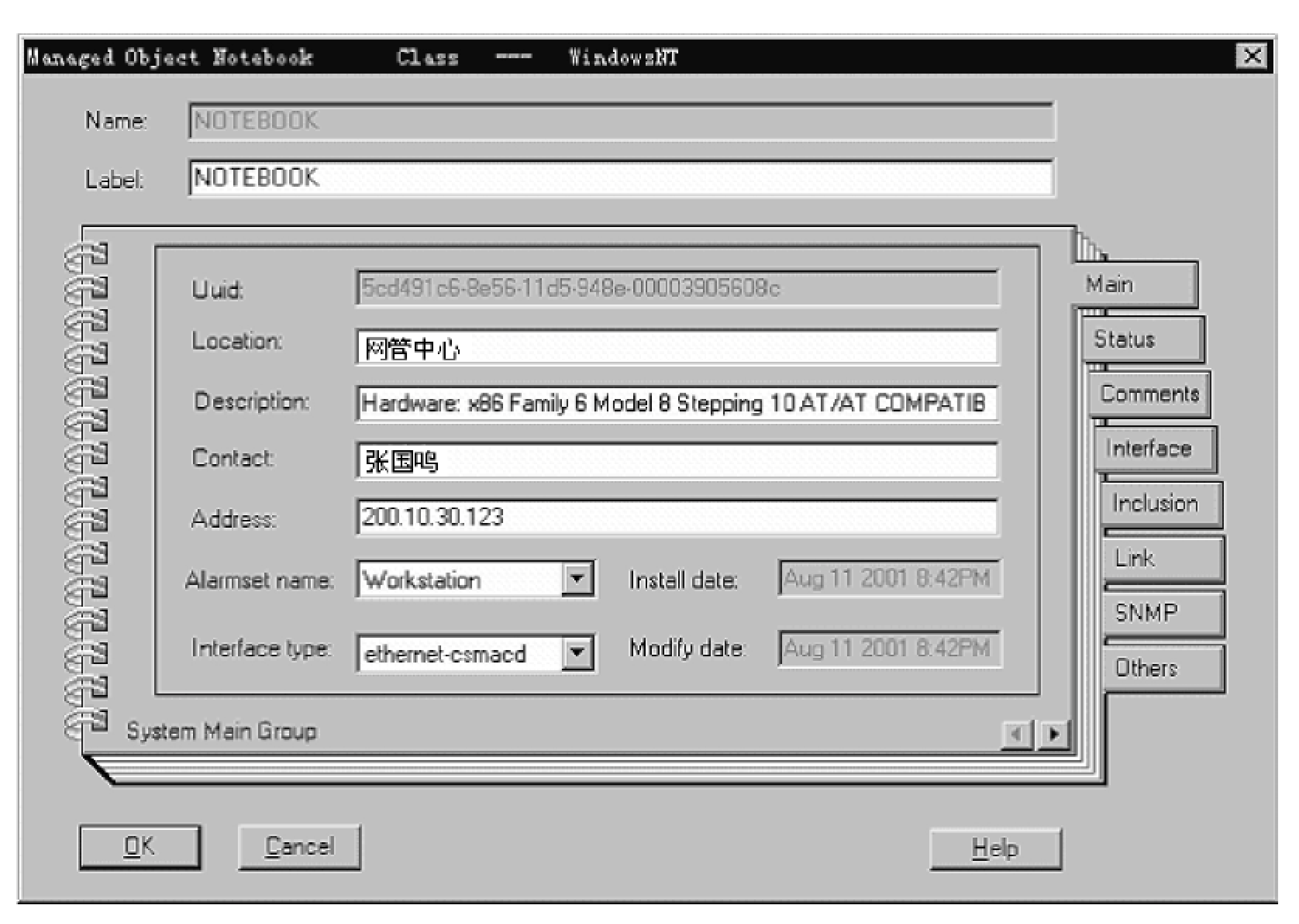


图 8-27　设备总体信息

网络设备上，单击鼠标右键，从弹出的快捷菜单中选择 Object View 子菜单，会弹出如图 8-29 所示窗口。

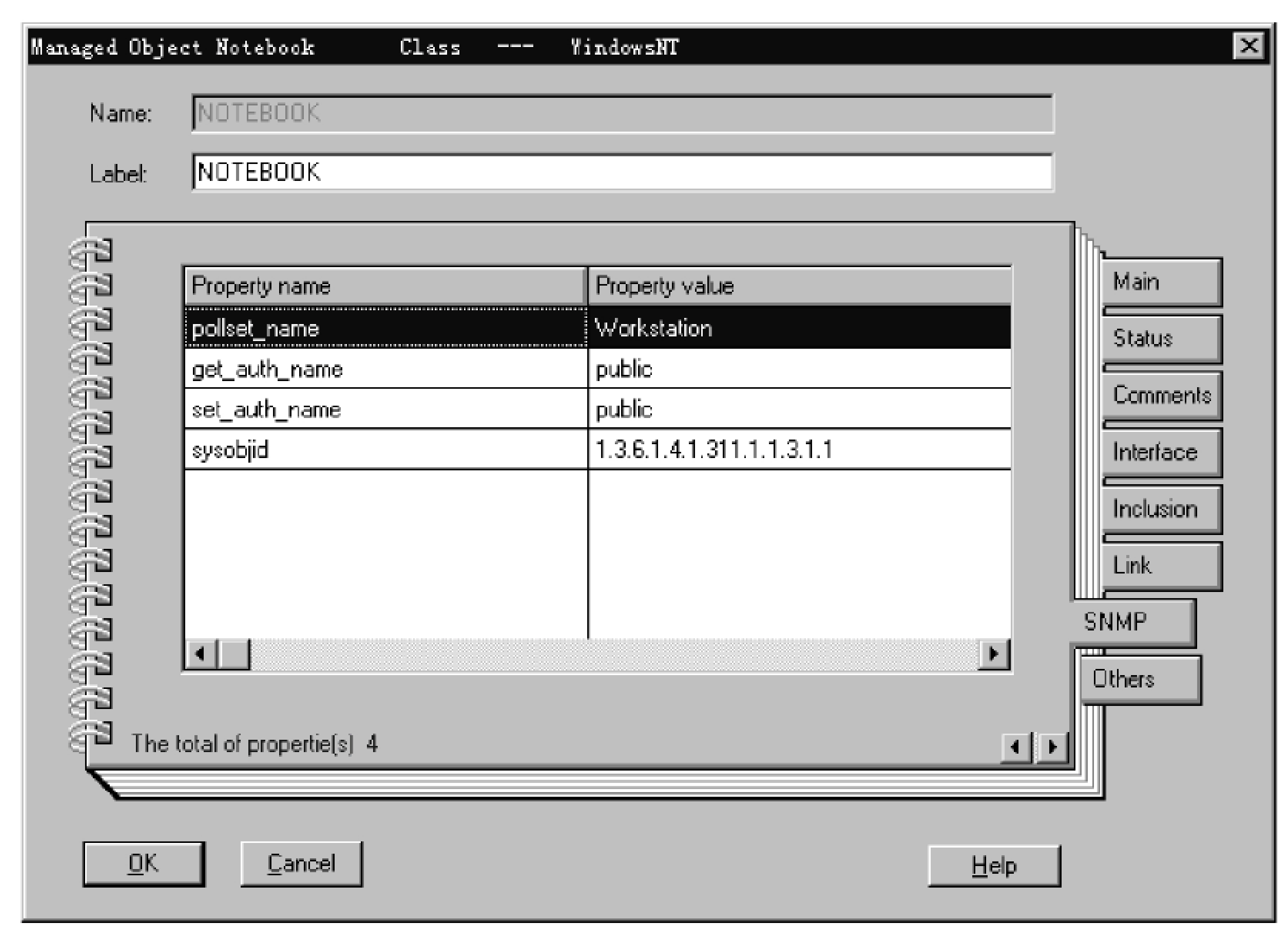


图 8-28 设备 SNMP 代理信息

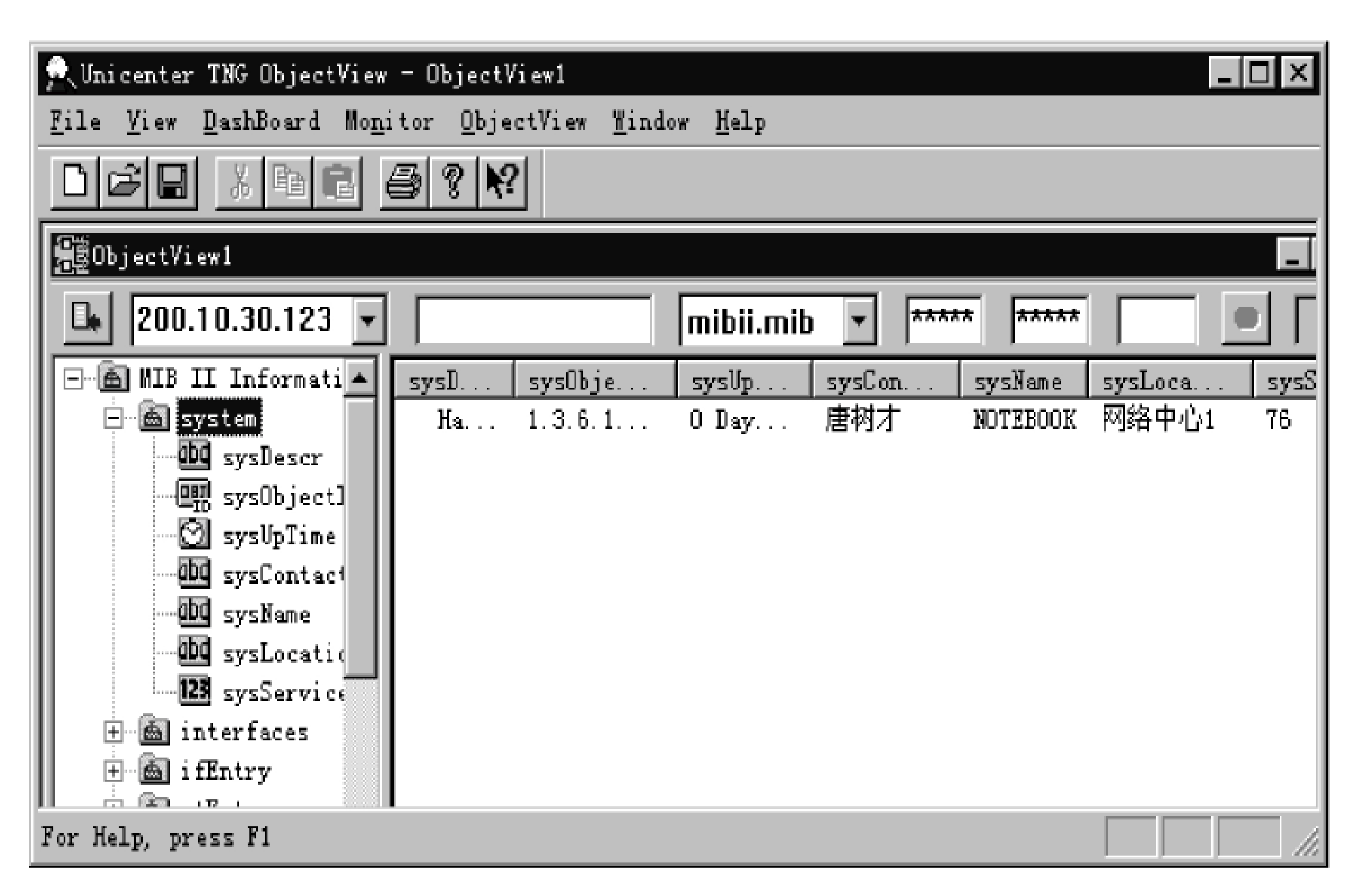


图 8-29 MIB-II 对象的信息

在该窗口中，可以查看设备中的所有 MIB-II 对象信息。如果对某个 MIB-II 对象不熟悉，可以通过该窗口查看该 MIB-II 对象的详细信息，方法是在图 8-29 所示窗口中选中某个 MIB-II 对象，单击鼠标右键，出现 Group Information 快捷菜单，选择该菜单，弹出该 MIB-II 对象组的信

息，如图 8-30 所示。通过该窗口，可以知道 System 组包含 7 个对象。

图 8-30　系统组对象

通过选择 Set Informat 单选按钮，可知道 System 组有 3 个可写对象，如图 8-31 所示。

前面讲过，Unicenter TNG 中提供了全新的三维虚拟现实界面使用户可以更直观地监控和管理分布在网络中的各种资源。方法是在程序组中选择 3D Map，可以进入三维虚拟现实世界，利用鼠标可以在三维环境中漫游，如图 8-32 所示。

在三维世界中单击鼠标，进入如图 8-33 所示的界面，通过该界面，可以知道目前网络中存在一个子网。

在该界面中，用鼠标选择该子网图标，一步一步可以进入该子网的三维世界，如图 8-34 所示。

在该窗口中，可以发现该子网中存在有 6 台网络设备，包括 2 台 Sun 设备、1 台 Windows NT 服务器、2 台 Windows NT 客户机、1 台网络打印机。通过该界面，还可以获得每个网络设备的详细信息，方法同二维图中的方法一致，这里不再赘述。

获得网络设备的另外一个方法是通过网络拓扑图，方法是在二维图形或三维图形界面中选择菜单 View 菜单下的 Topology Browser 选项，便可以获得网络的拓扑结构，如图 8-35 所示。

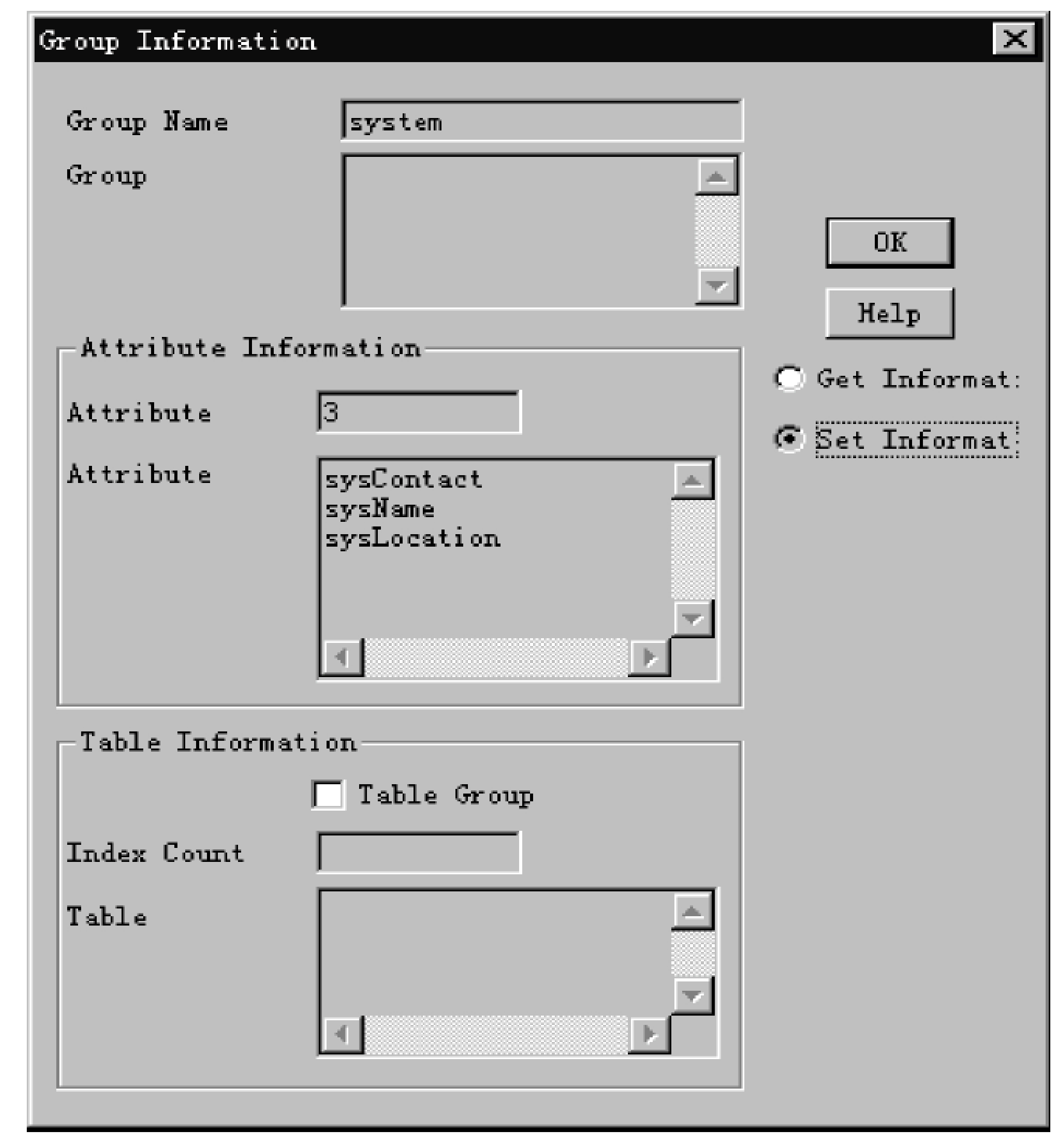


图 8-31　系统组可写对象

8.5.4　网络性能管理

利用 Unicenter TNG，不但可以监视网络上的被管理对象，而且还可以对这些对象的性能进行管理。Unicenter TNG 中有两个性能管理工具：一个是 ObjectView，另一个是 RMO。ObjectView 是实时测量单个网络部件性能的最佳工具。RMO（Response Management Option）可实现真正的端到端网络性能监控和对历史数据进行分析。

1. ObjectView

ObjectView 主要是一个性能工具。它基于代理对设备进行监视，提供得到的设备性能统计数据。它还可以提供基于设备 MIB 的配置信息。由于 ObjectView 考虑到了网络部件的测量以及隐藏在性能数据后面关系式的创建，使得这些数据即使对非技术人员来说都具有实际的意义。

ObjectView 通常用来进行网络性能的监视，如图 8-36 所示。图中给出了 ObjectView 连接的设备数、哪些接口关闭以及接收的数据包数。利用 ObjectView 提供的这些信息，可以很好地



图 8-32　三维世界



图 8-33　网络中有一个子网

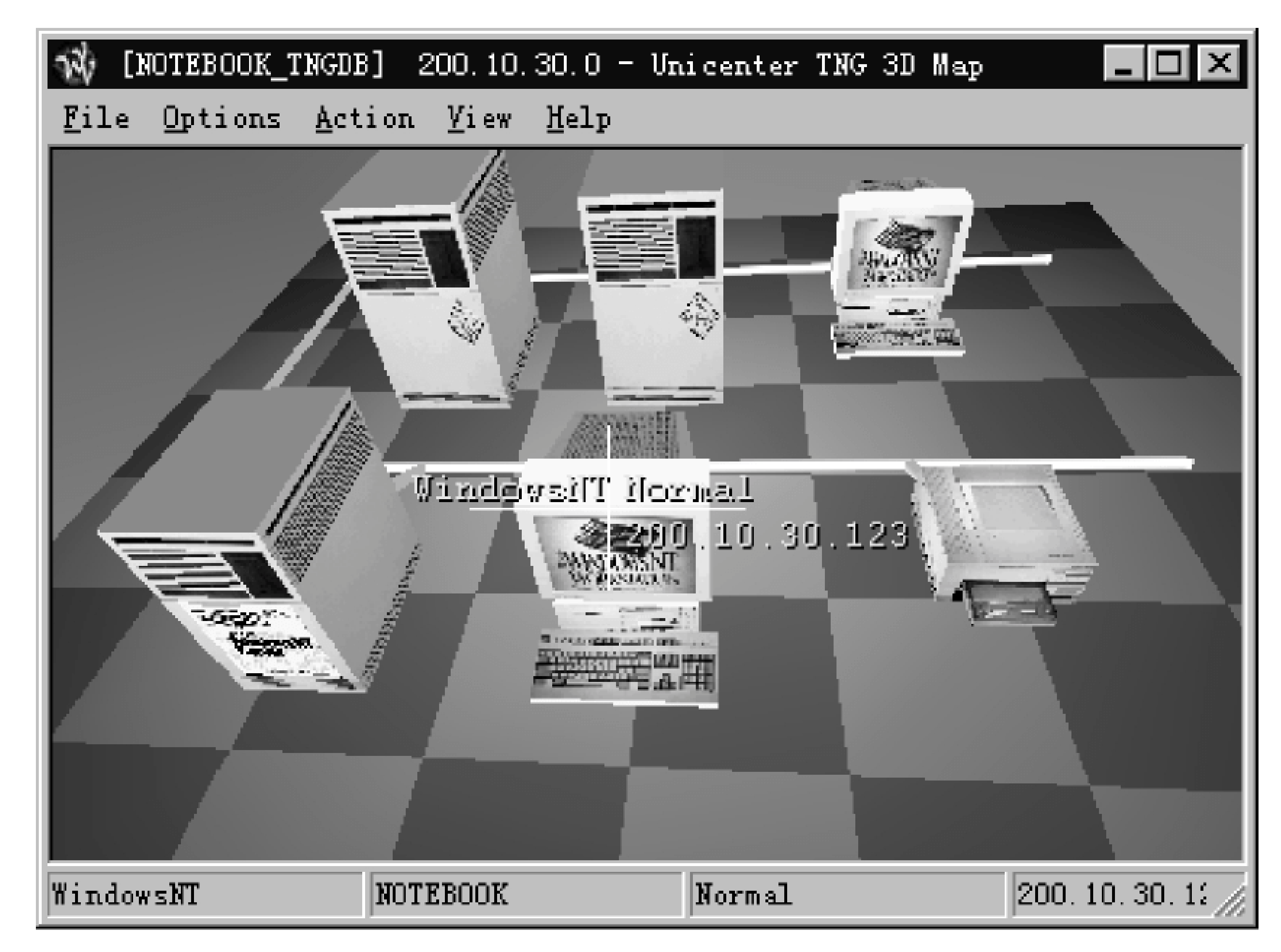


图 8-34 子网的三维世界

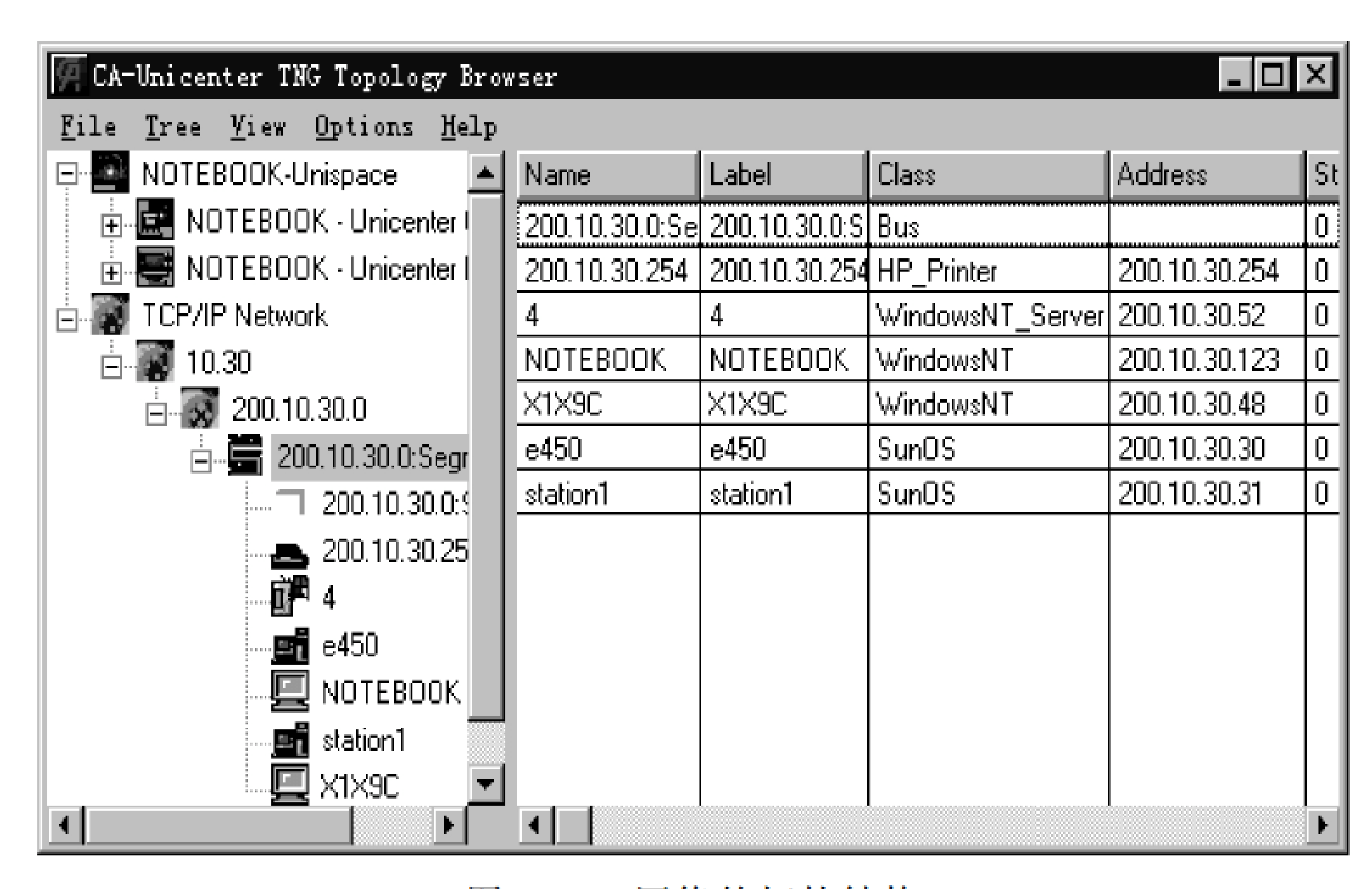


图 8-35 网络的拓扑结构

进行故障检测和性能的监视。

利用 ObjectView，系统管理员可以使用不同类型的图、标尺或者表格，可视化显示被监视的

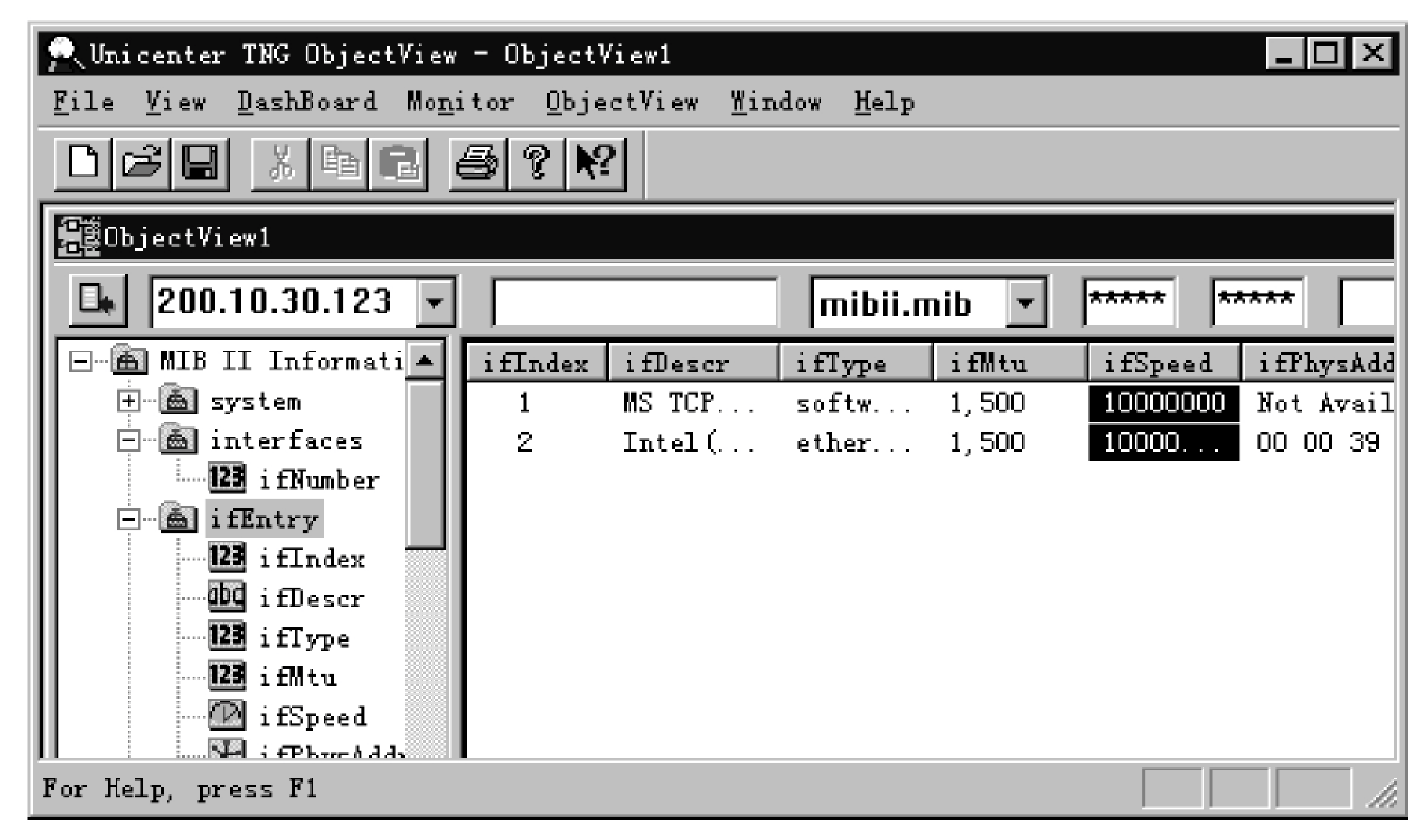


图 8-36　利用 ObjectView 监控网络性能

网络设备。系统管理员可以选择需要显示的属性，然后把它增加到 Excel 或者 ObjectView 仪表盘 ObjectView Dashboard 中，如图 8-37 所示。

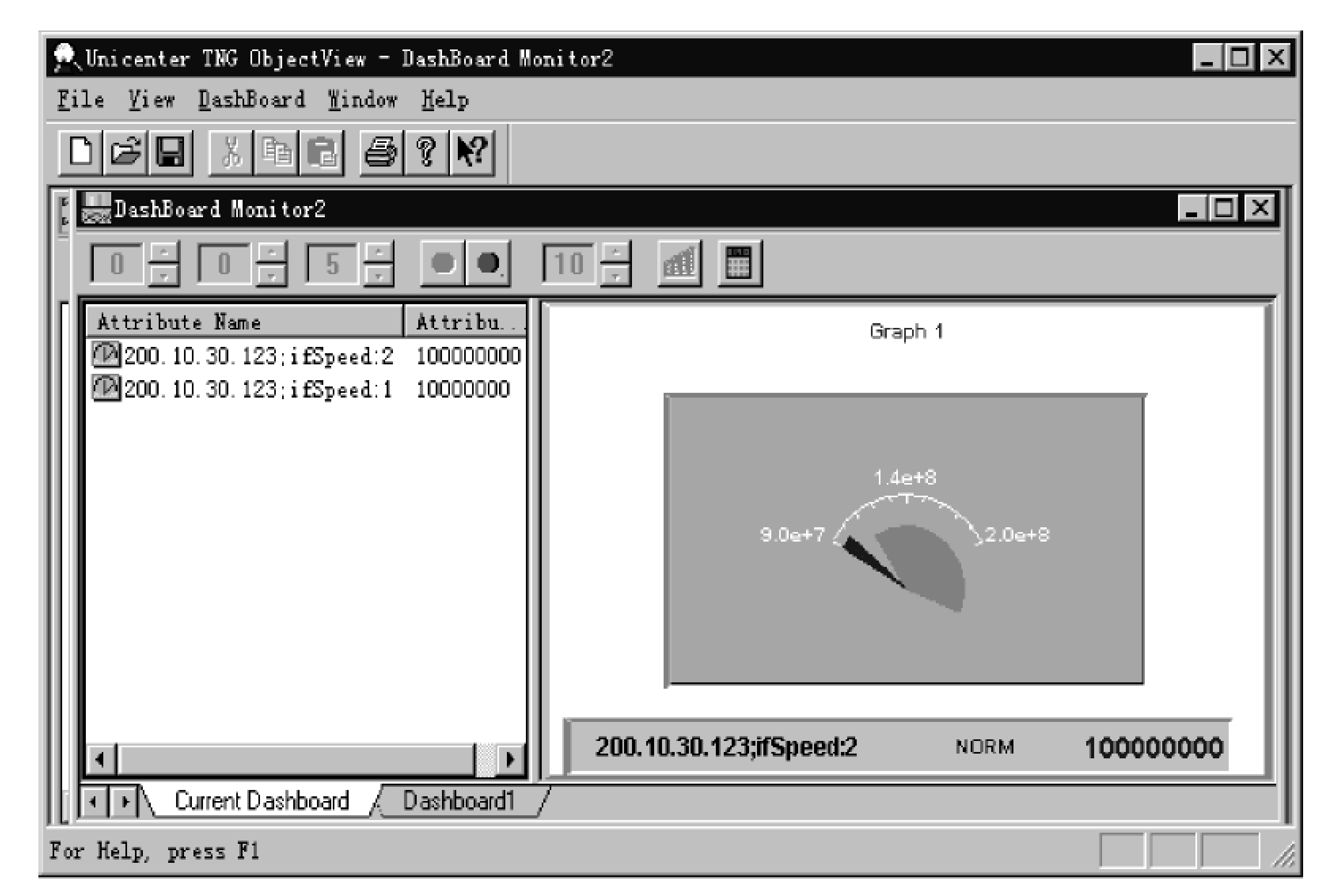
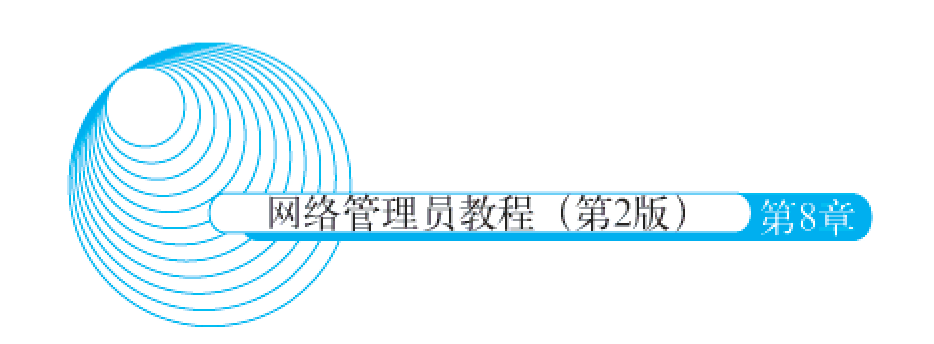


图 8-37　利用 Dashboard 可视化监视网络性能



2. Response Management Option(RMO)

Unicenter TNG 的 Response Management Option 是一个客户机/服务器分布式网络性能管理工具。它可以检测服务的级别、设备容量的使用以及局域网段和服务器的错误。它还可以提供以太网、广域网和 Cisco 路由器的相关信息。

RMO 的历史数据库和对象库共享对象标识器，这使得它能够直接使用 Unicenter TNG 对网络环境的检测结果，并能提供非 IP 网络资源信息，而且能够将性能警报直接送往 Unicenter TNG 的对象库，并显示在网络结构图上，还可以通过 Unicenter TNG 的 Event Browser 进行访问。

RMO 利用不同的服务器从不同的网络区域收集数据，因此它可以管理很大的网络环境。RMO 的历史数据库包含间隔数据和每天、周、月和年的综合数据。它还可以提供历史的和实时的数据报表。

RMO 的工作方式是监视客户机/服务器的应用程序以及网络软硬件，然后利用已经建立的服务级别协议对它们进行比较。通过收集安装在网络中的响应管理器 Response Manager 或者 SNMP 代理(使用 RMON 和 MIB Ⅱ数据)得到网络性能统计数据，如果发现没有达到预先设定的目标性能，RMO 会报错。RMO 还可以用来建立网络容量的分配计划。利用 RMO 的数据，可以决定在什么时间以及怎样迁移工作站，分割被过度使用的资源，扩充或者增加文件服务器，提供更加有效的网关等。

8.5.5 网络安全管理

Unicenter TNG Security Management 安全管理部件是一种基于策略的安全系统，与本地操作系统的安全联合发挥作用。它是一种外部安全策略，不取代本地操作系统的安全。安全策略定义了什么操作是允许用户做的，对资源(应用程序、文件、系统功能和登录等)的访问要通过安全策略来控制，在 Unicenter TNG 同意操作之后，再激活操作系统的安全，提供附加的检查。

Security Management 部件是企业管理部件的一部分，实时安全监测功能可防止攻击并且避免它们引起的损失。Security Management 的集成功能使得它能与企业管理部件功能协调工作。当检测到攻击时，触发事件，将事件发送到事件控制台的日志中去，并通知管理者。Security Management 的另一个特征是能够检测病毒，还能在检测到病毒时通知管理员。InocuLAN 是一个附加部件，它同 Unicenter TNG 一起，为服务器和客户机提供更强大的病毒检测功能。LnocuLAN 不但可以扫描普通文件，还可以扫描系统加载的压缩文件，当检测到病毒时，病毒将会被自动清除。应该说 LnocuLAN 是一种更高层次的病毒防护办法。

一次性登录(Single Sign-on)选项同 Security Management 一起，为在多个系统上注册的用户提供了一种有效的工具。用户不必记住不同的密码和登录过程，一次性登录选项允许用户只登录一次，通过鼠标单击就能访问用户授权的多个系统。每个系统的登录过程对于用户都是透

明的。

作为企业管理部件的一部分，Security Management 在初始安装时安装。安装完 Unicenter TNG 后，Security Management 就可以使用了，但它只提供一些基本的安全管理功能。要扩展并提高它的能力，还要通过下面的附加步骤来完成。

(1) 检查安全管理选项和服务器/客户机参数选择。选择与需求相关的选项，并设置与环境相协调的值。

(2) 将本地操作系统上的用户 ID 信息加入安全管理数据库。

(3) 验证安全策略。

(4) 激活安全策略。

8.6 网络管理技术的新发展

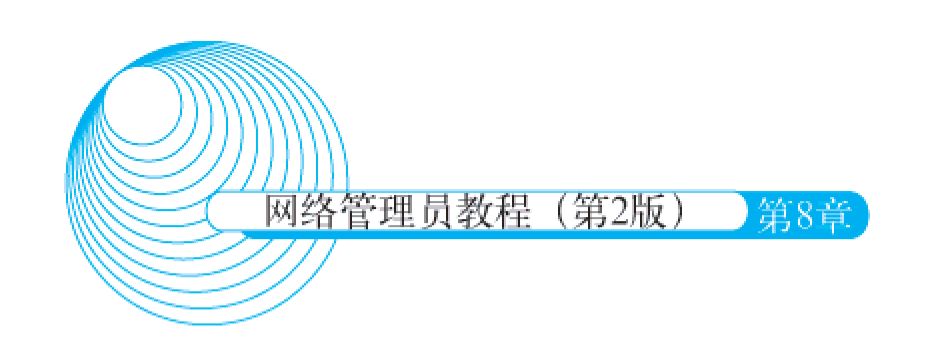
8.6.1 网络管理技术的发展趋势

在过去的十几年中，由于 IT 技术的迅速发展，网络正在向智能化、综合化、标准化发展。先进的计算机技术、全光网络技术、神经网络技术正在不断地应用到网络中来，这也给网络管理提出了新的挑战。未来的网络管理应该进一步融入高新技术，建立成熟的网络管理标准，加快促进网络管理的一体化、智能化和标准化进程。

与网络技术本身日新月异的发展相比，网络管理技术的进步显得有点步履维艰。功能单一、配置复杂、缺乏标准、耗资巨大是广大用户普遍不满的主要原因。

现行的网络管理技术大都属于第三层管理，其致命弱点是支持的网络设备不全，尤其是缺乏对交换型局域网以及广域网的有效支持。这类技术一般是通过安装在 LAN 中各个网络设备上的代理软件收集有关状态信息，经汇总后提交网络管理人员进行处理。为此，网管产品开发商们都在想方设法研究改进措施。例如：HP OpenView 不但支持更多类型的网络设备，还能对交换机进行管理，并得到了 400 多家硬件厂商的支持。这些厂商在向用户提供 Windows 或 UNIX 下的驱动程序的同时，还提供面向 OpenView 的网管代理软件。通过与 Riversoft 达成的协议，HP 将在 OpenView 中内嵌 Riversoft 的网络管理操作系统（NMOS）。Riversoft 公司是一家研发第二层网络管理技术产品的公司，该公司的高层人士认为，NMOS 可能会成为第二层网络管理技术事实上的标准。据权威机构估计，NMOS 能使网络崩溃的概率平均降低 65%。在与 HP 结盟之后，Riversoft 又相继与 Cisco、Intel 达成类似的协议，将其软件延伸至下一代无线网络管理和未来新的网络应用服务管理领域。

还有一些厂商通过其他办法来实现网络的第二层管理。Entuity Eye 公司的网管产品将第二层管理特性与网络性能分析相结合，将影响网络性能的所有不同参数集成在一个监视窗口中。每个端口、设备和网段都有其对应的“状态百分值”，或称“性能下降总指数”，该指数可以将



网络的动态状况精确地告诉网管人员。

随着因特网技术的快速发展，应用服务供应商（ASP，Application Service Provider）应运而生，由ASP向广大用户提供配置、租赁、管理应用解决方案等多项服务。利用连接到因特网的服务器宿主应用程序，ASP的客户通过Web浏览器能够随时、随地与远程可管理应用模块或应用软件包交互。但问题是：由于网络管理产品的技术标准迟迟不能确立，给ASP和用户带来了很多麻烦。虽然ASP服务商向用户提供了服务监视软件，用户可以借此确认所花的钱是否真的得到了相应的服务。但是，如果监视软件与用户其他管理软件不能很好地集成，那么该软件的性能和准确性就要大打折扣。作为一种过渡，很多厂商在产品研发中正向一种“概念信息模型”靠拢，并通过XML语言实现不同厂家产品的沟通，例如CiscoWorks 2000。尽管XML语言不会实现各厂商产品间的彻底兼容，但它毕竟为各种产品间的对话提供了一种可行的手段。

网络的远程管理已不是什么新鲜东西，但最新的远程管理技术能让网络管理人员通过个人数字助理（PDA，Personal Digital Assistant）设备，或采用无线应用协议（WAP，Wireless Application Protocol）的移动设备实现对网络的管理。但这种远程管理其实还是受限的，这取决于网络故障部位或故障性质还能否为远程管理者提供一个基本的管理支持环境。因此，让网络自行发现运行中的问题，自动排除一些网络故障，即将人工智能引入网络管理技术，这是开发商们一个新的研究方向。该系统能对各种网络故障进行判断，并具有自学习功能。Smarts公司已在其Incharge系列网管产品中加入了人工智能技术。该产品实际上是专家系统的变体，基于既定的规则算法，是一种比较古老的人工智能技术。与传统的专家系统不同的是，Incharge能够根据其所工作网络场所的不同自动进行升级，因此，可以动态提升其性能。

随着网络种类的繁荣及网络技术的提高，网络管理工作日益复杂，未来的网络管理强调更好的接入控制，即加强不同用户、多媒体业务功能的管理。同时，人工智能技术将应用于网络管理，未来的网络管理系统还将具有自学习能力和自我规划功能。现在，网络管理越来越受到人们的重视，相信随着IT技术的进步，网络管理技术将逐渐成熟并日臻完善。当然，无论网络管理技术进步到何种程度，都不能奢望出现让网络管理人员一劳永逸的网管工具。网络管理本身是一项极其复杂的工作，网管工具要考虑的问题比让计算机下棋或管理飞机的进出港要复杂得多。即使有了带有人工智能的网管工具，它也仅仅让网络管理变得容易一些，而不会全部代替人的工作。

8.6.2 基于Web的网络管理

作为一种全新的网络管理模式，基于Web的网络管理模式，被简称为WBM（Web-Based Management）。WBM从出现伊始就表现出强大的生命力，它以其特有的灵活性、易操作性等特点赢得了许多技术专家和用户的青睐，被誉为是“将改变用户网络管理方式的革命性网络管理解决方案”。

1．WBM 简介

随着企业内部网(Intranet)的快速发展,其本身的结构也变得越来越复杂,同时也大大增加了网络管理的工作量,给网络管理员真正管理好内部网带来了很大的困难。传统的网络管理方式已经不适应当前网络发展的趋势。为此,基于 Web 的网络管理 WBM 模型应运而生。

一般内部网都运行于 TCP/IP 协议之上并且通过防火墙将其与外部因特网隔离。网络内部都建有 Web 服务器,它们通过与超文本标记语言(HTML,Hypertext Markup Language)有关的协议与其他用户通信。内部网用户可以在任何一个网络节点或是网络平台上使用友好的、易操作的 Web 浏览器与服务器进行通信。除此以外,管理员还发现了 Web 技术的其他益处,例如,Browser/Server 计算模式与传统的 Client/Server 计算模式相比,更利于优化网络配置和降低网络扩展、维护费用。因为 Web 浏览器对计算机的硬件要求很低,因而管理员可以把很多的计算和存储任务转移到 Web 服务器上去完成,而允许用户依靠简单、廉价的计算平台去访问它们。这种“瘦客户机/胖服务器”模式降低了硬件要求并且提供给用户更大的灵活性。在网络管理领域,包括 IBM/Tivoli、Sun、HP 和 Cisco 等公司在内的主要网管系统供应商都竞相推出融合了 Web 技术的管理平台。

简单地讲,基于 Web 的网络管理 WBM 模型是在内部网不断普及的背景下产生的。内部网实际上就是专用的 World Wide Web,以 Web 服务器组建而成,主要用于组织内部的信息共享。内部网用户通过简单、通用的操作界面 Web 浏览器可以在任何地点的任何网络平台上与服务器进行通信。WBM 模型就是将内部网技术与现有的网络管理技术相融合,为网络管理人员提供更具有分布性和实时性,操作更方便、能力更强的管理网络系统的方法。

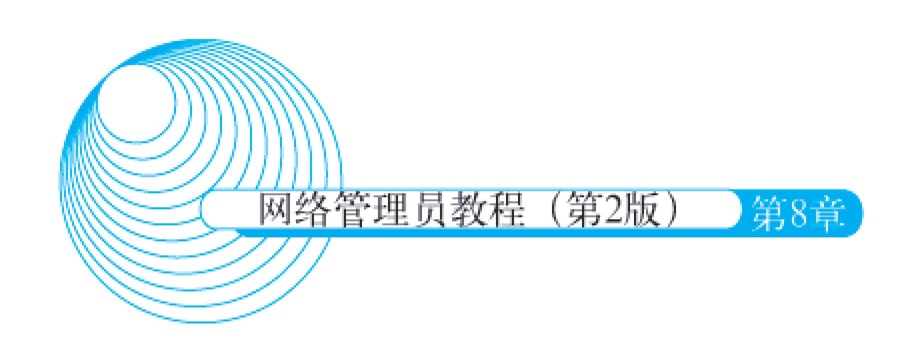
WBM 网络管理模型的主要优点有:

(1) 提供了地理上和系统上的可移动性。而 WBM 可以使网络管理员通过 Web 浏览器从内部网的任何一台工作站上进行网络管理的有关操作。对于网络管理系统的管理者来说,在一个平台上实现的管理系统服务器,可以从任何一台装有 Web 浏览器的工作站上访问,工作站的硬件系统可以是专用工作站,也可以是普通 PC 机,操作系统的类型都不受限制。

(2) 具有统一的网络管理程序界面。网络管理员不必像以往那样学习和运用不同厂商的网络管理系统程序的操作界面,而是通过简单而通用的 Web 浏览器进行操作,完成网络管理的各项任务。

(3) 网络管理平台具有独立性。WBM 的应用程序可以在各种环境下使用,包括不同的操作系统、体系结构和网络协议,无须进行系统移植。

(4) 网络管理系统之间可无缝连接。管理员可以通过浏览器在不同的管理系统之间切换,比如在厂商 A 开发的网络性能管理系统和厂商 B 开发的网络故障管理系统之间切换,使得两个系统能够平滑地相互配合,组成一个整体。



2. WBM 的标准

为了降低网络管理的复杂性、减少网络管理的成本，WBM 管理的开放式标准必不可少。有两个 WBM 的标准目前正在酝酿之中，一个是 WBEM（Web-Based Enterprise Management）标准，另一个是 JMAPI（Java-Management Application Program Interface）标准。

1）WBEM

基于 Web 的企业管理标准 WBEM 是由 Microsoft 公司最初提议的，目前已经得到了 6 家网络厂商的支持。WBEM 是一个面向对象的工具，各种抽象的管理数据对象通过多种协议（如 SNMP）从多种资源（如设备、系统、应用程序等）中收集。WBEM 能够通过单一的协议来管理这些对象，被定位成“兼容和扩展”当前标准（如 SNMP 协议、DMI 协议和 CMIP 协议等），而不是替代它们。尽管 WBEM 事实上是一个 Web 应用，但它的真正目标是对所有网络元素和系统进行管理，包括网络设备、服务器、工作平台和应用程序。

WBEM 旨在提供一个可伸缩的异构的网络管理机构。它与网络管理协议如 SNMP、DMI 兼容。WBEM 定义了网络管理的体系结构、协议、管理模式和对象管理器，管理信息采用 HTML 或其他因特网数据格式，使用 HTTP 传输请求。

2）JMAPI

Java 管理应用程序接口 JMAPI（Java Management Application Programming Interface），是 Sun 公司作为它的 Java 标准扩展 API 结构而提出的。JMAPI 的目标是解决分布系统管理的问题。JMAPI 是一种轻型的管理基础结构，它对被管资源和服务进行抽象，提供了一个基本类集合。除去字面上的意思外，JMAPI 更是一个完全的网络管理应用程序开发环境。它提供了一张功能齐全的特性表，其中包括：创建特性表、图表的用户接口类；基于 SNMP 的网络 API；远程过程调用的结构化数据访问方式和类型向导等。

开发人员可以利用 JMAPI 实现具有完整性和一致性的公共管理，并可以通过对 JMAPI 的扩展，满足特定网络管理应用的需要。JMAPI 不仅仅是一个类库的集合，它还具有独特的网络管理体系结构。JMAPI 由浏览器用户界面、管理运行模块和被管元素 3 个部件组成。其中浏览器界面是管理人员进行管理操作的界面，用来管理视图模块、被管对象接口和支持 Java 的浏览器；管理运行模块对被管对象进行实例化，是整个管理的核心，由 HTTP 服务器、被管对象工厂、代理对象接口和通报分发器组成；被管元素指被管理的系统和设备，由代理对象构成。

现在人们花费许多精力扩展 Web 的范围和能力。但要让 Web 真正应用于网络管理，以取代传统的网络管理模式，还需要国际标准组织、网络设备供应商、网络管理系统供应商和用户做大量的基础工作。随着计算机网络和通信规模的不断扩大，网络结构日益复杂和异构化，网络管理也随之迅速发展。由传统的网络管理系统发展到基于 Web 的网络管理系统已经是时代不可逆转的潮流。网络在发展，网络管理也在发展，Web 技术正在悄悄地改变着网络管理的方式，

让我们拭目以待 WBM 技术的发展。

3．WBM 的实现方式

有两种基本方案可以实现 WBM。一种是基于代理的解决方案，另一种是嵌入式解决方案。

1）基于代理的解决方案

基于代理的 WBM 方案是在网络管理平台之上叠加一个 Web 服务器，使其成为浏览器用户的网络管理的代理者，网络管理平台通过 SNMP 或 CMIP 与被管设备通信，收集、过滤、处理各种管理信息，维护网络管理平台数据库。WBM 应用通过网络管理平台提供的 API 接口获取网络管理信息，维护 WBM 专用数据库。管理人员通过浏览器向 Web 服务器发送 HTTP 请求来实现对网络的监视、调整和控制。Web 服务器通过 CGI 调用相应的 WBM 应用，WBM 应用把管理信息转换为 HTML 形式返还给 Web 服务器，由 Web 服务器响应浏览器的 HTTP 请求。基于代理的解决方案如图 8-38 所示。

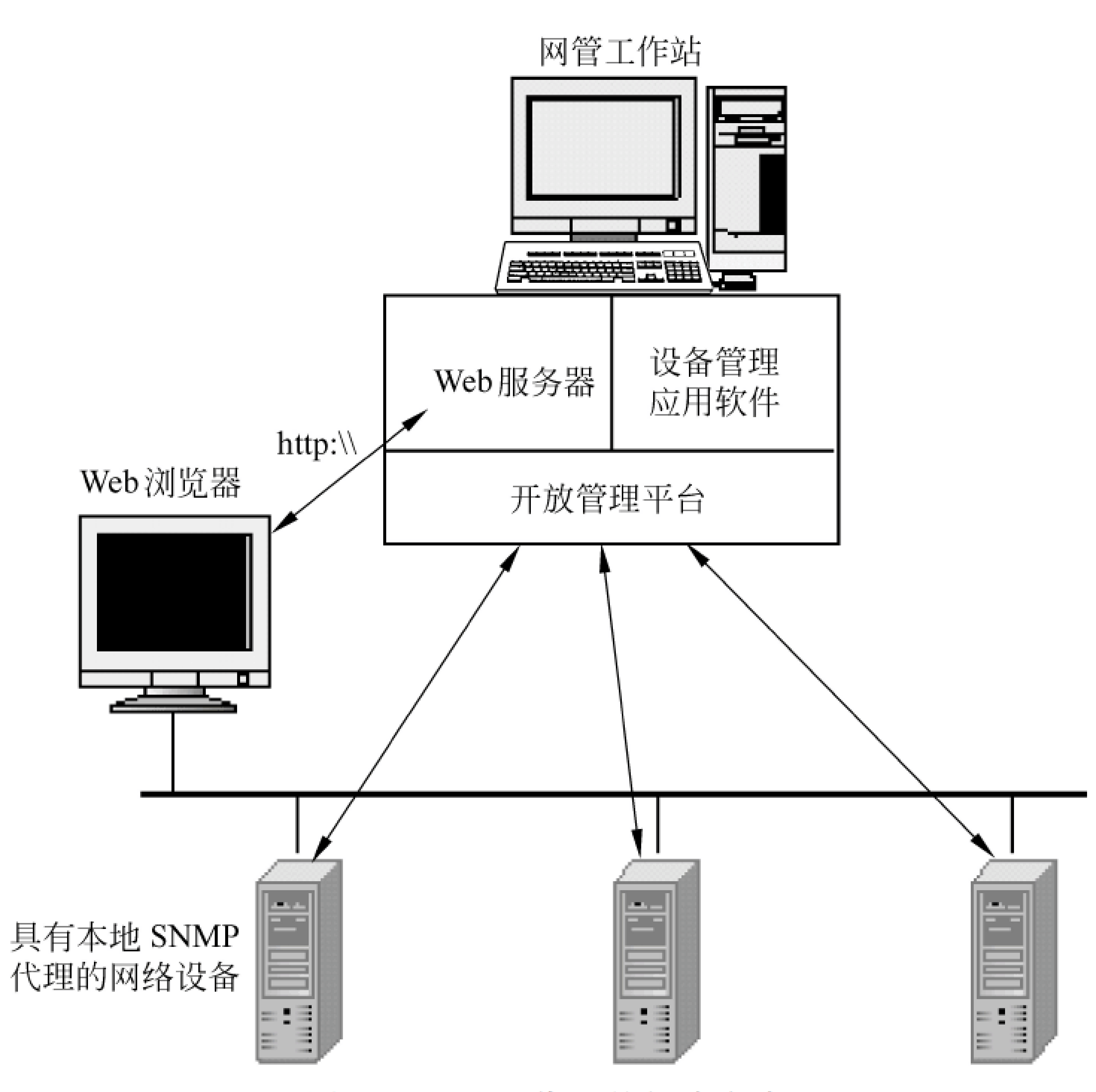
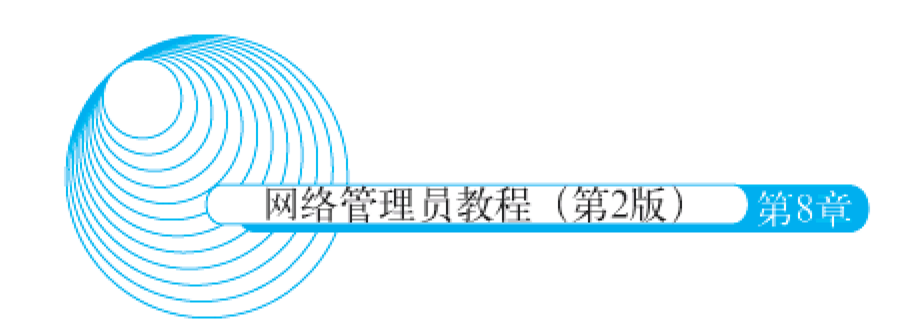


图 8-38　基于代理的解决方案

基于代理的 WBM 方案在保留了现存的网络管理系统的特征的基础上，提供了操作网络管理系统的灵活性。代理者能与所有被管设备通信，Web 用户也就可以通过代理者实现对所有被



管设备的访问。代理者与被管设备之间的通信沿用 SNMP 和 CMIP，因此可以利用传统的网络管理设备实现这种方案。

2）嵌入式解决方案

嵌入式 WBM 方案是将 Web 能力嵌入到被管设备之中。Web 服务器事实上已经嵌入到终端网络设备内部。每一个设备都有自己的 Web 地址，这样网络管理员就可以通过用 Web 浏览器和 HTTP 协议直接访问设备的地址来管理这些设备。代理的解决方案继承了基于工作站的管理系统和产品的所有优点，此外它还具有访问灵活的特点。因为代理服务器和所有的网络终端设备通信仍然通过 SNMP 协议，因而这种解决方法可以和只支持 SNMP 协议的设备协同工作。从另一方面来看，内嵌服务器的方法带来了单独设备的图形化管理。它提供了比命令行和基于菜单的 Telnet 接口更简单易用的接口，能够在不牺牲功能的前提下简化操作。嵌入式 WBM 方案如图 8-39 所示。

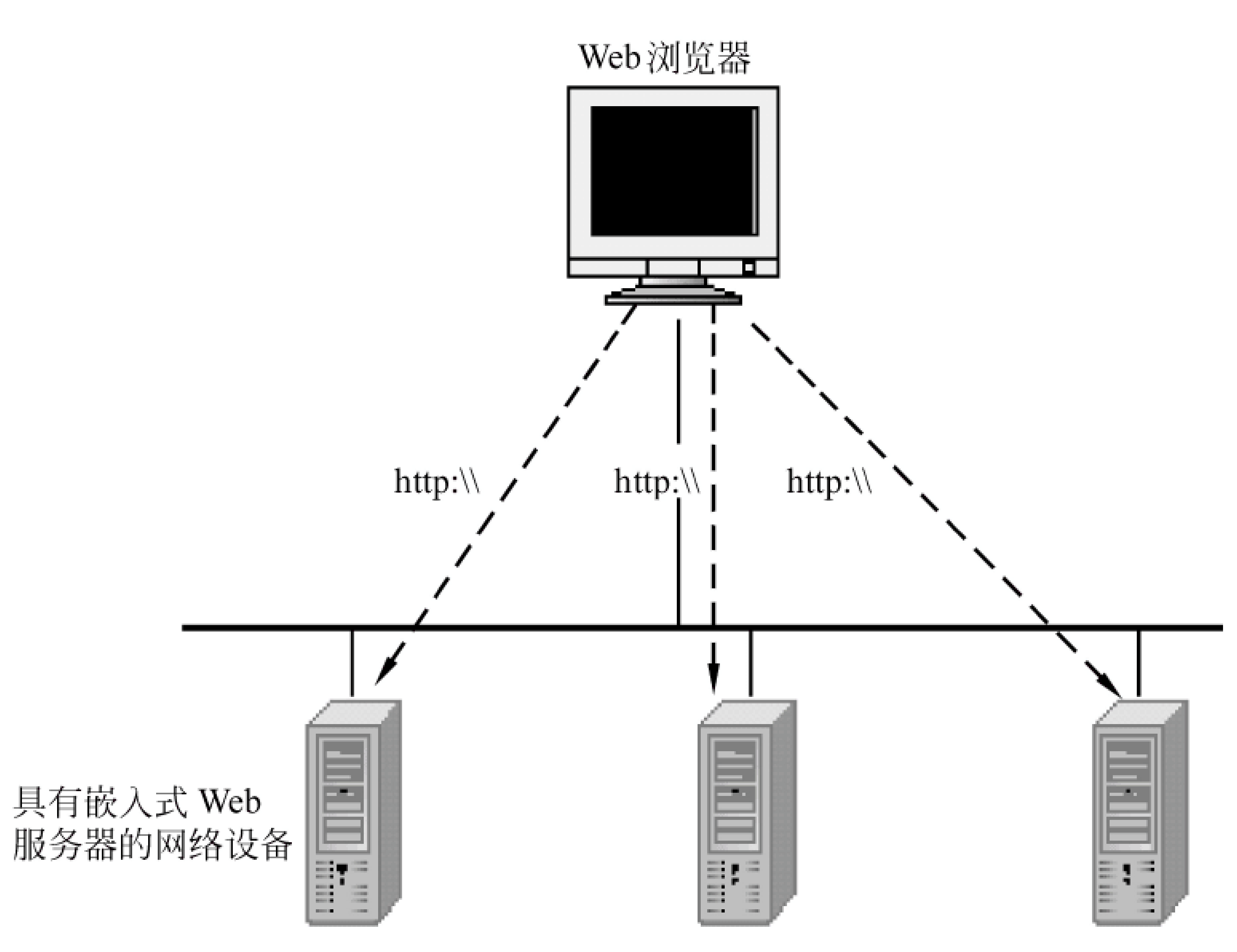


图 8-39　嵌入式解决方案

嵌入式 WBM 方案给各个被管设备带来了图形化的管理，提供了简单的管理接口。网络管理系统完全采用 Web 技术，如通信协议采用 HTTP 协议，管理信息库利用 HTML 语言描述，网络的拓扑算法采用高效的 Web 搜索、查询点索引技术，网络管理层次和域的组织采用灵活的虚拟形式，不再受限于地理位置等因素。

嵌入式 WBM 方案对于小型办公室网络来说是理想的管理方式。小型办公室网络相对来说比较简单，也不需要强大的管理系统和整个企业的网络视图。由于小型办公室网络经常缺乏

网络管理和设备控制人员，而内嵌 Web 服务器的管理方式则可以把用户从复杂的管理中解脱出来。另外，基于 Web 的设备实现了真正的即插即用，减少了安装时间和故障排除时间。

未来的内部网中，基于代理和嵌入式的 WBM 方案都将被采用。一个大型的机构可能需要采用代理方案进行全网的监测与管理，而且代理方案也能充分管理大型机构中的 SNMP 设备。同时，嵌入式方案也有强大的生命力，它在界面以及设备配置方面具有很大优势。特别是对于小规模的环境，嵌入式方案更具优势，因为小型网络一般不需要强大的管理系统。嵌入式的 WBM 方案由于提供了高度改良的接口，因而使企业网络安装和管理新设备更加方便。如果将以上这两种方式混合使用，则更能体现二者的优点。

4. 实现 WBM 的关键技术

实现 WBM 的技术有多种，最常用的是使用描述 WWW 页面的语言 HTML。HTML 可以构建页面的显示和播放信息，并可以提供对其他页面的超链接，图形和动态元素（如 Java Applet）也可以嵌入到 HTML 页面中。因此用 HTML 页面提供 WBM 的用户信息接口是很理想的。

WBM 的另一个关键技术是通过 Web 浏览器访问数据库。传统的 Web 不能直接访问数据库，但随着数据库发布技术的进步，这个问题已经得到了解决。现在已经有多种 Web 访问数据库的技术，其中公共网关接口（CGI，Common Gateway Interface）技术得到了较多的应用。CGI 提供了基于 Web 的数据库访问能力。当 WBM 应用程序需要访问 MIB 时，可以利用 CGI 对数据库进行查询，并格式化 HTML 页面。

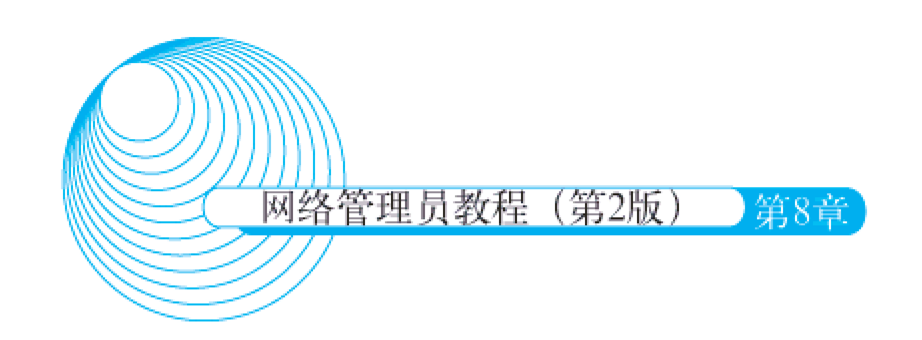
对 WBM 来说，还有一个重要的技术，那就是 Java 语言。它是一种解释性程序语言，也就是在程序运行时，代码才被处理器程序解释。解释器语言易于移植到其他处理器上。Java 的解释器是一个被称为 Java 虚拟机（JVM）的设备，它可以应用于千变万化的处理器环境之中，而且可以被绑定在 Web 浏览器上，使浏览器能够执行 Java 代码。Java 提供了一套独立而完备的程序 Applet 专用于 Web。Applet 能够被传送到浏览器，并且在浏览器的本地机上运行。Applet 具有浏览器强制安全机制，可以对本地系统资源和网络资源的访问进行安全控制。

Java Applet 对于 WBM 中的动态数据处理是一种有效的技术。它能够方便地显示网络运行的画面、集线器机架等图片，也能实时表示从轮询和陷阱得到的更新信息。

Java 在 WBM 中还有一种应用就是如果将 JVM 嵌入到一个设备之中，该设备就可以执行 Java 代码。利用这一点，可以将应用程序代码在工作站和网络设备之间动态地传递。

5. WBM 中的安全性考虑

WBM 的安全性对于网络本身的安全是至关重要的。一个安全的 WBM 系统要能够保证网络管理信息的保密性、完整性和真实性。保密性不仅涉及网管信息存放，更重要的在于网络管



理信息的传输。信息的完整性是指通过网络对信息进行增删改，以及对信息进行传递时，要保证相关信息不能残缺不全或被人有意篡改。信息的真实性主要是指对通信双方的身份进行认证和鉴别，以防止对系统的非法访问、对信息的破坏以及通信双方对信息的真实性发生争议。

由于 WBM 控制着网络中的关键资源，因此不能容许非法用户对它的访问。一个安全的网络需要有防火墙将其与因特网隔离开，以保护企业内部网的资源，比如防止未经许可的外部访问运行 WBM。出于安全考虑，对服务器的访问可以通过口令控制和地址过滤来控制。从这个角度来看，WBM 也是一个基于服务器的需要保护的设备，只有内部网上的授权用户才能访问 WBM 系统。基于 Web 的设备在向用户提供易于访问的特性的同时，也可以限制用户的访问。管理员可以对 Web 服务器加以设置以使用户必须用口令来登录。网络管理员可能认为有些网络数据是敏感的，因而需要加密。通过使用 Web，只须在服务器简单地启用安全加密，用户就可以加密从浏览器到服务器的所有通信数据。服务器和浏览器就可以协同工作来加密和解密所有传输的数据，这相对于 SNMP 和 Telnet 的安全性而言，已经是一个不小的进步。WBM 方式并不和已经存在的安全性方式相冲突，如已经在 Windows 和 UNIX 中应用的目录结构、文件名结构等。另外，网络管理员还可以很方便地使用目前十分有效的安全技术来加强 Web 系统的安全，如数字签名、消息认证和身份认证等技术。

此外，Java Applet 的安全问题对 WBM 也很重要。因为 Java Applet 将字符串和数据暴露在光天化日之下，因此存在着被篡改的危险。尽管 Java Applet 具有一些安全保障措施，如被规定不能写盘、破坏系统内存或生成至非法站点的超级连接，但仍需要对其代码进行保护，以保证收到的 Java Applet 与原作完全相同。

8.6.3 基于 CORBA 技术的网络管理

CORBA（Common Object Request Broker Architecture）的中文意思是公共对象请求代理体系结构。CORBA 是对象管理组织（OMG，Object Management Group）为解决分布式处理环境下硬件和软件系统的互连互通而提出的一种解决方案。CORBA 的核心是对象请求代理 ORB。在分布式处理中，它接收客户端发出的处理请求，并为客户端在分布环境中找到实施对象，令实施对象接收请求，向实施对象传送请求的数据，对实施对象的实现方法进行处理，并将处理结果返回给客户。通过 ORB，客户端不需要知道实施对象的位置、编程语言、远程主机的操作系统等信息，即可实现对实施对象的处理。

简单地说，CORBA 是一个面向对象的分布式计算平台，它允许不同的程序之间透明地进行相互操作，而不用关心对方位于何地、由谁来设计、运行于何种软硬件平台以及用何种语言来实现等。CORBA 分布式对象技术正在逐渐成为分布式计算环境发展的主流方向，使用分布对象技术开发的系统具有机构灵活性、软硬件平台无关性、系统可扩展性等优点，特别适用于网络环境下的分布式系统开发，能够有效地解决异构环境下的应用互操作性和系统集成。

OMG已经提出了基于CORBA的网管系统的体系结构，使用CORBA的方法可以实现基于OSI开放接口和OSI系统管理概念。可以预见，CORBA将在网络管理和系统管理中占有越来越重要的位置。自从OMG确定了CORBA规范的1.1版本以来，CORBA技术不断吸收各种新的思想，不断加以优化，CORBA 2.0规范的推出，实现了真正意义上的互操作性。

然而，CORBA在进一步扩大其应用领域的过程中，其局限性也逐渐暴露出来，例如，实时系统、服务质量、高速性能系统、多媒体应用以及事件的优先权排序和事件过滤等，CORBA都不能直接为这些应用提供服务。为此，CORBA3.0规范被推出，以弥补在以往应用中的局限性，CORBA3.0增加了一些新的特性：分布式组件模型(CORBA Component Model)与脚本语言、值传对象(OBV)、可移植对象适配器(POA)规范、异步消息规范、服务质量控制QoS、实时CORBA、与因特网技术的整合等。

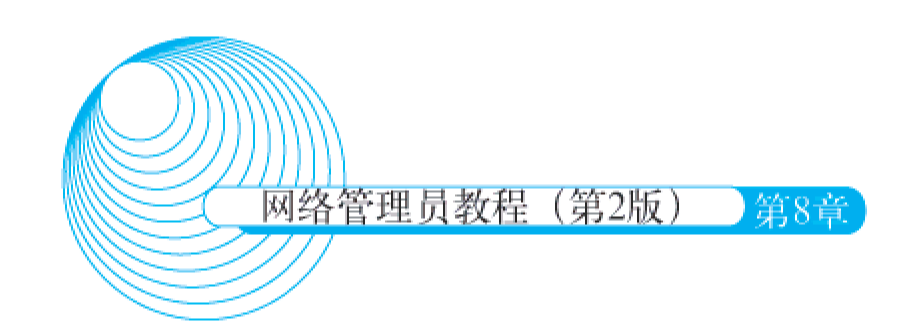
在网络和系统管理的实现中较有影响的模型是SNMP和CMIP，这两个模型各有其优点，但同时又都存在着不足之处。通过前面的学习知道，SNMP在因特网上被广泛接受，它最主要的一个特点就是简单，但是在需要完成十分复杂的管理任务时，它就不能充分满足要求。许多通信厂商的网络结构是基于CMIP的，但是CMIP受到自身过于复杂以及标准化过程太慢的限制，至今仍未获得像SNMP那样广泛的支持。可以预见，这两种管理体系框架在很长时间内将会同时存在。

随着面向对象的分布式处理模型的出现，CORBA作为第三种解决方案被提出。CORBA提供了统一的资源命名、事件处理以及服务交换等机制。虽然它最初的提出是针对分布式对象计算，而并非针对网络管理任务的，但是在很多方面它都适合于管理本地的以及更大范围的网络。与现有的模型相比，CORBA提供的功能比SNMP更强大，而且不像CMIP那么复杂。此外，CORBA支持C++、Java等多种被广泛使用的编程语言，因此它已经迅速被大量的编程人员所接受。通过CORBA，他们可以使自己的程序具有分布式的特点，而且不必在逻辑上有很大的变动。正因为如此，现在普遍认为，CORBA将会在网络管理和系统管理中占有越来越重要的位置。

利用CORBA进行网络管理，既可以用CORBA客户实现管理系统，也可以利用CORBA来定义被管对象，还可以单独利用CORBA实现一个完整的网络管理系统。但是为了发挥现有网络管理模型在管理信息定义以及管理信息通信协议方面的优势，一般是利用CORBA实现管理系统，使其获得分布式和编程简单的特性，而被管系统仍采用现有的模型实现。因此，目前讨论基于CORBA的网络管理，主要是解决如何利用CORBA客户来实现管理应用程序，以及如何访问被管资源，而不是如何利用CORBA描述被管资源。目前的问题是研究SNMP/CORBA网关和CMIP/CORBA网关，以支持CORBA客户对SNMP或CMIP的被管对象进行管理操作。

8.6.4 基于主动网的网络管理

传统网络的主要作用是在终端系统之间进行信息的传递，而对传递的信息内容并不关心。



为了完成信息传递任务，需要进行一些处理。但这些处理仅限于对"分组头信息"进行解释，或执行电路的信令协议。这些处理的主要目的是选择路由、控制拥塞和保证服务质量 QoS。由于这些处理是在用户提出通信请求之后进行的，因此网络是"被动"发挥作用的。在现有的网络管理模型（如 CMIP、SNMP）中，采用管理者—网管代理模式，网管代理也是根据管理者的操作命令被动地工作。这使得管理者必须采用轮询的方式不断地访问代理者，这一方面增加了网络的业务量负荷，同时也限制了网络管理的实时性。

主动网技术就是让网络的功能成分更加主动地发挥作用。为此，它允许用户和各交换节点将自己订制的程序注入网络，在网络中主动寻找发挥作用的场所。为了能够执行用户注入的程序，要求交换节点具有对流经的数据内容进行检查并执行其中所包含的程序代码的能力。

在网络管理中应用主动网技术对解决现行网络管理模型中存在的问题很有帮助。例如，可以根据网络的运行情况，动态地移动网络管理中心，使其更接近网络的心脏部位，以减小网络管理的时延，降低传递管理信息的业务量。又比如，可以设计具有特定功能的主动网分组，在分组中插入特定代码，使其成为网络管理的"巡逻兵"，在网络节点之间移动，监视网络中的异常情况。也可以让主动网分组携带处理故障的程序代码，一旦遇到特定的故障，便可及时调整故障节点状态，而不必等待管理中心的处理。

应用主动网技术进行网络管理已经引起了人们的重视，并正在逐步地应用于网络管理系统之中。现在已经提出了几种基于主动网技术的分布式网络管理模型，其中，比较有代表性的是：

- 委派管理（MBD，Management By Delegation）模型。
- 移动代理（MA，Mobile Agent）模型。

8.6.5 TMN 网络管理体系的发展

近十几年来，在全世界范围内，电信技术、电信市场在不断进步、扩大。为降低网络成本，网络运营商引入多厂商设备，在得到利益的同时，也增大了电信网络管理的复杂程度。同时，为向用户提供高质量、高可靠性的电信服务，增强企业竞争能力，有效降低网络运营成本，电信运营商需要采用更先进的技术和自动化的管理手段进行支撑。因此，电信网络运行维护管理的重要性日益突出。面对日益复杂的电信网络及多种电信业务，传统的电信网络管理系统因为没有标准的互连接口，相互之间难以协调互通，难以共享网络及信息资源，已经不能适应现代电信网络运营管理的需要。在这种情况下，国际电信联盟 ITU-T 于 1985 年提出了电信管理网（TMN，Telecommunications Management Network）的概念。

TMN 的基本概念是提供一个有组织的网络结构，以取得各种类型的运行系统之间、运行系统与电信设备之间的互连，是采用商定的具有标准协议和信息的接口进行管理信息交换的体系结构。TMN 的目标是提供一个电信管理框架，采用通用网络管理模型的概念、标准信息模型和标准接口完成不同设备的统一管理。提出 TMN 体系结构的目的是管理异构网络、业务和设备，

支撑电信网和电信业务的规划、配置、安装、操作及组织。从技术和标准的角度来看，TMN是一组原则和为实现原则中定义的目标而制订的一系列的技术标准和规范。

TMN逻辑上区别于被管理的网络和业务，这一原则使TMN的功能可以分散实现。这意味着通过多个管理系统，运营者可以对广泛分布的设备、网络和业务实现管理。从逻辑上看，TMN是一个由各种不同管理应用系统，按照TMN的标准接口互连而成的网络。这个网络在有限的点上与电信网接口，与电信网是管与被管的关系。

TMN的复杂度是可变的，从一个运营系统与一个电信设备的简单连接，到多种运营系统和电信设备互连的复杂网络。TMN在概念上是一个单独的网络，在一些点上与电信网相通，以发送和接收管理信息，控制它的运营。TMN可以利用电信网的一部分来提供它所需要的通信。

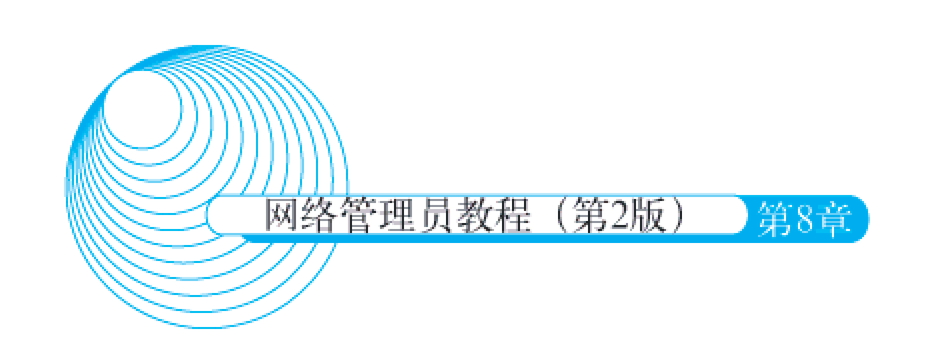
TMN采用OSI管理中的面向对象的技术对组成TMN环境的资源以及在资源上执行的功能块进行描述。

TMN通过丰富的管理功能跨越多厂商和多技术进行操作。它能够在多个网络管理系统和运营系统之间互通，并且能够在相互独立的被管网络之间实现管理互通，因而互联的和跨网的业务可以得到端到端的管理。TMN为电信网络和业务的管理提供信息传送、存储和处理的手段。TMN可以提供管理端到端的电信业务所需要进行的信息交换的手段，所有类型的电信网和网元，如模拟网、数字网、公众网和专用网中的交换系统、传输系统、电信软件、网络的逻辑资源（如电路、通道或由其他资源支持的电信业务）都可能是一个电信管理网的管理对象。理论上对于TMN的应用领域并不限制，因为TMN的建议还在不断的开发之中，但是许多应用领域的实际情况会限制TMN的实施。

TMN自提出至今已有十几年，其本身也在不断地发展和完善。TMN标准的制订及研究方向与电信业的建设发展、运营管理方式、管理要求都有着十分密切的关系。TMN目前向以下几个趋势发展。

（1）从网络管理向业务管理过渡。从用户的角度出发，各电信用户直接接触的是电信业务，关心的是电信运营商提供业务的质量；从电信运营商的角度出发，电信运营商所运营的网络最终目的是提供给各用户满意的业务及服务质量，不断扩大市场，提高竞争能力。因此，在市场驱动下，各电信运营商正在逐步从网络管理向业务管理过渡。业务管理包括：快速的业务引入和应用、多种业务的选择、高质量的客户服务以及管理自身网络的能力等。目前，ITU-T等组织正在从事业务管理领域的标准研究，其中包括：电子传单、故障单、安全管理、电信运营者内部故障单的交换、业务申请单交换、业务配置、业务监视、性能监控和计费应用等。

（2）对异构系统进行综合管理。网络信息必须能够从网元管理层EML经由网络管理层NML传递到业务管理层SML和事务管理层BML，这样高层才能获取准确的网络信息并据此作出相应决策，决策信息再反向传递给各个管理层。在多厂商环境下，网络运营系统之间、采用不同技术的网络管理系统之间应能够互操作。这样，才能从单一的接口获取端到端的网络数据，



网络故障才能被正确定位及自动解除。

（3）TMN 实现的技术在不断发展。这主要体现在以下几个方面：公共管理信息协议 CMOT 作为遗留的 Q3 协议栈框架而被接受；TINA-C 与对象管理组织 OMG 正在发展分布式的 TMN，初步形成开放分布式处理（ODP，Open Distributed Processing）与开放分布管理体系（ODMA，Open Distributed Management Architecture）的方法和理论；独立于具体技术的操作平台正在发展中，例如：采用 Java 管理应用程序接口的 API（JMAPI）技术，采用 HMMS/P（Hyper Media Management Schema/Protocol）的 WEBM 技术，与 Java 结合的 CORBA 技术等。

（4）电子传单（Electronic Bonding）逐步应用。遗留系统与用户系统之间的内部连接通过 Manager/Agent 及公共的数据标准，应用电子传单技术的 X 接口可以完成连接功能。ATIS（Alliance for Telecommunication Industry Solutions）与网络管理论坛 NMF 正在从事故障单、本地号码可携、业务签署等方面的研究工作。

8.6.6 智能化的网络管理

1. 基于专家系统的网络管理

1）专家系统的分类

专家系统技术是最早被应用于网络管理的智能技术，并且已经取得了很大的成功。专家系统能够利用专家的经验和知识，对问题进行分析，并给出专家级的解决方案。专家系统从功能上可以定义为在特定领域中具有专家水平的分析、综合、判断和决策能力的程序系统。它能够利用专家的经验和专业知识，像专家一样工作，在短时间内对提交给它的问题给出解答。

在网络管理中运用的专家系统按功能大致分为 3 类：维护类、提供类和管理类。维护类专家系统提供网络监控、障碍修复、故障诊断功能，以保证网络的效率和可靠性；提供类专家系统辅助制订和实现灵活的网络发展规划；管理类专家系统辅助管理网络业务，当发生意外情况时辅助制订和执行可行的策略。

在实际应用的系统中，维护类专家系统占绝大多数。这类系统的大量应用，已经在大型网络的日常操作中产生了重要作用；现有的提供类专家系统大多数用于辅助网络设计和配置，最近也出现了用于辅助网络规划的系统；最常见的管理类专家系统是辅助进行路由选择和业务管理的系统，即在公共网络中监视业务数据和加载路由表，以疏导业务解除拥塞。除此之外也开发了一些特殊用途的系统，如逃费监察系统等。

专家系统要处理的问题可分为综合型和分析型两类。综合型问题是如何在给出元素和元素之间的关系的条件下进行元素的组合。这类问题常在网络配置、计费和安全中遇到。分析型问题是从总体出发考察各元素与总体性能之间的关系。这类问题常在网络故障诊断和性能分析中遇到。对分析类问题常采用“预测”和“解释”两种分析方法。预测法根据网络中各网络元

素的性能推测网络的总体性能，是网络性能分析的常用方法。解释法则根据观察到的网络元素及其性能推测网络元素的状态，是网络故障诊断的常用方法。

网络管理专家系统有脱机和联机两种类型。脱机型专家系统是简单的类型。当发现网络存在问题以后，利用脱机型专家系统解决问题。专家系统根据询问网络的配置情况和观察到的状态，对得到的信息进行分析，最后给出诊断结果和可能的解决方案。脱机型专家系统的缺点是不能实时地使用，只能用于问题的诊断，而网络是否已经发生问题却要先由人来判断。联机型专家系统与网络集成在一起，能够定时监测网络的变化状况，分析是否发生了问题以及应该采取什么行动。

2）专家系统的能力

专家系统一般由知识库、规则解释器（推理机）和数据库 3 部分组成。

知识库中存放“如果：＜前提＞，于是：＜后果＞”形式的各种规则。

数据库中存放事实（如系统的状态、资源的数量）和断言（如系统性能是否正常）。当＜前提＞与数据库中的事实相匹配时，规则将让系统采取＜后果＞中指示的行动，通常是改变数据库中的断言，或向用户提问将其回答加到数据库中。

网络管理专家系统在满足网络管理的任务和要求的同时，还应具备下列几种能力：

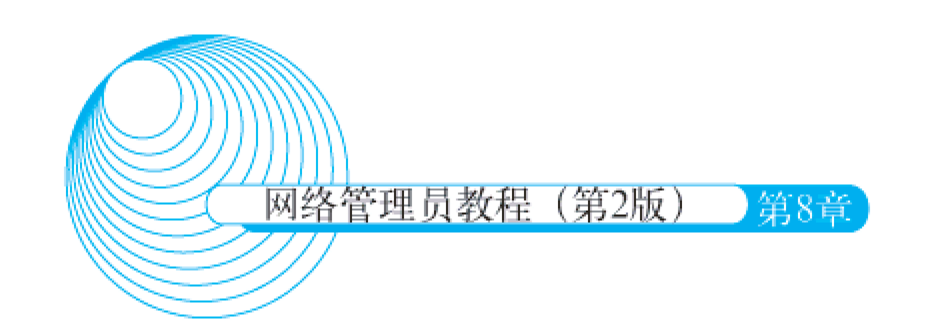
（1）具有处理不确定性问题的能力。网络管理就是要对网络资源进行监测和控制。为了完成这个任务，网络管理专家系统不仅需要了解网络的局部状态，还要了解网络的全局状态。但是这一点是很难满足的，因为网络的状态时刻都在变化，由于状态信息的获取和传递需要时间，当状态信息提供给专家系统时，有些已经过时了。这就是说，网络管理专家系统只能根据不完全和不确切的信息进行推理。

（2）具有协作能力。由于网络管理任务很重，需要的功能也很多，因此在一个网络管理系统中往往需要有多个网络管理专家系统，每个专家系统面向特定的功能领域。由于在管理中，不同功能领域中的功能相互之间是有关系的，这就需要网络管理专家系统也要有相互协作的能力。

（3）具有适应分布变化的能力。网络是一个不断变化的分布式系统，网络管理专家系统必须能够适应这一特点。联机的网络管理专家系统要利用现有网络管理模型中的轮询机制及时地获取网络的最新状态，以便及时发现问题和给出解决方案。

3）专家系统的应用

目前，应用最广的是故障管理专家系统。故障管理包含 3 个相关的功能：故障检测、故障诊断和故障修复，这也是专家系统所要提供的功能。故障检测包括通过检测数据进行故障告警和根据性能数据预测故障两个方面。故障检测的基本功能就是识别并忽略那些表面异常但对检测没有参考意义的信息，以减少错误告警。这样的能力普通人是不具备的，而有经验的专家却能作出准确的判断；故障诊断包括故障的确认和定位。为此系统要采取多种措施，包括运行诊



断程序、分析性能统计数据、检查日志等，通过历史数据和当前数据进行推理判断，这些工作可以由专家系统进行指导和完成；故障修复中的一个问题是如何使故障产生的损失最小。解决这个问题既要考虑本地的情况，也要考虑全网的情况。为了尽快恢复业务，需要选择业务的恢复路由。这些问题往往难以通过解析的方法获得满意的解决，而专家的经验和知识却十分有效。利用专家系统，可以对不同的方式进行权衡，使故障修复的措施得到优化。

在配置管理中，资源分配的优化是一个非常复杂的问题。即使对于规划设计阶段的“静态”网络，诸如如何分配交换机以及骨干网的容量等问题也要花费大量的研究资金和人力。将专家系统用于网络规划设计中的优化资源分配已经取得了成功。对于运行中的“动态”网络，预先确定的资源分配优化规则往往不能提供理想的网络配置方案。专家系统除了支持预先确定的针对偶然事件的处理策略外，还可采用启发式的方法提供比较理想的网络配置方案。

在性能管理中，通过监测到的性能数据对网络的性能状态进行分析是一项复杂的工作。单纯采用解析的方法是不够的，一般需要有专家的分析和判断。这类专家系统需要着重研究专家系统的数据驱动问题和网络在不同性能指标下的状态变化。性能分析专家系统应能察觉网络在进入低性能甚至故障之前的细微变化，以便及时采取启动故障管理或性能管理的功能，减小和避免损失。为了能够发现这样的细微变化，专家系统需要支持基准状态的和不可接受状态的两种操作。

在安全管理领域，也有许多适合于专家系统发挥作用的场合。通过建立专家级的访问控制规则保护网络资源以及网络管理系统便是典型的应用。普通的防火墙系统通过设定严格的访问控制规则来保护网络资源，但这种做法常常会使一些合法的操作也受到限制。而专家系统的方法便于设定智能的灵活的访问控制规则，既严格有效地阻止非法侵入，又不对合法操作产生限制。

计费管理是目前唯一没有采用专家系统技术的领域。但这并不说明专家系统在这个领域没有用武之地。也有人因此批评计费领域保守，有一种观点是现在计费系统的自动化水平已经很高，即使采用专家系统使其继续有所提高，但其安全性令人顾虑。

2. 基于智能 Agent 的网络管理

1）智能 Agent 的概念

智能 Agent 不仅仅是一个代理者，而是一个非常宽的概念。它泛指一切通过传感器感知环境，运用所掌握的知识在特定的目标下进行问题求解，然后通过效应器对环境施加作用的实体。这类实体具有下述特性：

（1）自治性。Agent 的行为是主动的、自发的，Agent 有自己的目标或意图。根据目标、环境等的要求，Agent 对自己的短期行为作出计划。

（2）自适应性。Agent 根据环境的变化自动修改自己的目标、计划、策略和行为方式。

（3）交互性。Agent 可以感知其所处的环境，并通过行为改变环境。

（4）协作性。Agent 通常生存在有多个 Agent 的环境中，Agent 之间良好有效的协作可以大大提高整个多 Agent 系统的性能。

（5）交流性。Agent 之间可以采用通信的方式进行信息交流。任务的承接、多 Agent 的协商、协作等都以通信为基础。

由以上对比可以看出，由 Manager 和 Agent 两个角色共同构成的网络管理实体所具有的能力，仅是智能 Agent 能力的一小部分。因此，用智能 Agent 来代替标准网络管理模型中的管理实体 Manager 和 Agent，是在现有的网络管理框架下，实现智能化的一个很好的方案。

分布式人工智能中的智能 Agent 是由知识和知识处理方法两部分组成的。知识是其自身可以改变的部分，而知识处理方法是其自身不可改变的部分。它的显著特征是“知识化”，因而被称为智能 Agent。

2）智能代理网络管理结构

智能代理网络管理（IANM，Intelligent Agent Network Management）系统由通信接口、智能控制器、MIB 接口和知识库构成。通信接口接收外部环境的管理信息（来自其他 IANM 的请求及通报），由智能控制器根据这些管理信息及其自身的状态，进行分析和推理，产生控制命令，通过 MIB 接口将控制命令变成对被管对象的操作，操作结果通过 MIB 接口返回智能控制器，然后通过通信接口向发来请求的 IANM 报告。上述活动与现有的 Agent 的活动是十分相像的。但是，除此之外更重要的活动是，IANM 可以自治地检测环境（被管对象及其自身的状态），经过分析推理后，对环境进行调整和改造，必要时与其他 IANM 通信联络。

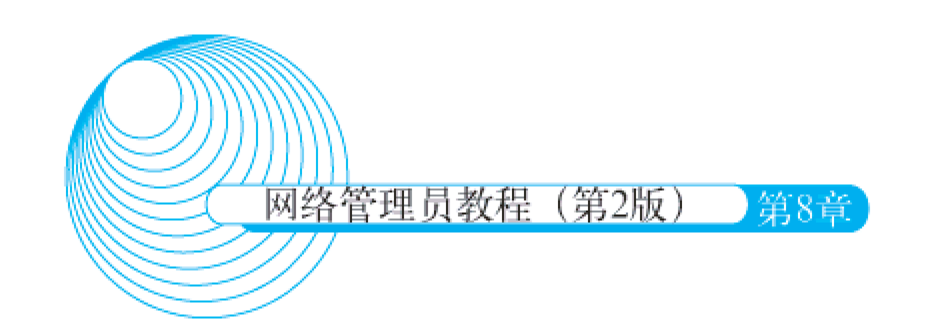
3）基于 IANM 的网络管理模型

在基于 IANM 的网络管理模型中，每个网络节点配置一个 IANM，用于管理本地 MIB 和向本地的网络管理应用提供服务。IANM 之间通过通信网络和 Agent 通信协议相互通信，在必要时进行协同工作和远程监控。这个模型与现有的标准网络管理模型的主要区别是大部分网络管理任务依靠 IANM 和本地网络管理应用可以在本地自治完成，而不必将管理信息传递到管理者处进行集中处理。只是在需要多 IANM 协同工作和远程监控时，才通过通信网络传递管理信息。因此这是一个分布式的、自治的、协同工作的网络管理模型。实现这样的模型，可以有效地降低网络中传递管理信息的负荷，提高网络管理的实时性。

3．基于计算智能的宽带网络管理

1）计算智能简介

宽带网络具有业务种类多、容量大、处理速度快等特点。对于网络管理来说，业务种类多的特点显著提高了业务量控制的难度；容量大的特点要求网络要有很高的可靠性和存活性，故障自愈技术成为关键技术；处理速度快的特点要求网络管理的算法要有实时性，否则便无法与网络的数据传输速率相匹配。在功能方面，业务量控制、路由选择和故障自愈是宽带网络管理需



要特殊研究和开发的3项关键技术。在研究和开发中，基于传统方法的技术遇到了很大的困难，主要有两个原因：一是业务种类多导致了综合业务特性过于复杂，传统的方法难以处理；二是实时性要求高，不适合采用复杂的解析方法。

在这种背景下，基于计算智能的方法受到了重视。计算智能是人工智能的一个重要分支，与传统的基于符号演算模拟智能的人工智能方法相比，计算智能是以生物进化的观点认识和模拟智能。按照这一观点，智能是在生物的遗传、变异、生长以及外部环境的自然选择中产生的。在用进废退、优胜劣汰的过程中，适应度高的结构被保存下来，智能水平也随之提高。因此说计算智能就是基于结构演化的智能。

计算智能的主要方法有人工神经网络、遗传算法和模糊逻辑等。这些方法具有自学习、自组织、自适应的特征和简单、通用、适于并行处理的优点。由于具有这些特点，计算智能为研究和开发上述宽带网络管理中的关键技术提供了方法。

2）基于神经网络的CAC

呼叫接纳控制（CAC，Calling Admit Control）要根据对新呼叫和现有连接的QoS、业务量特性的分析来进行。然而，在大型ATM网络中这种分析是非常复杂和耗时的。因为业务种类繁多，QoS各异，并且因业务的同步关系、比特速率、连接模式、种类（话音、数据、视频、压缩与非压缩、成帧与非成帧）等都不尽相同，混合起来的业务更是十分复杂。解决这类问题，需要具有高速运算机制和对各种复杂情况的自适应能力的方法。人们提出了基于3层前馈神经网络和反向传播学习算法（BP，Back Promulgate）的CAC模型，为在大型ATM网络中实现自适应CAC提供了一个较好的候选方案。

前馈神经网络是相对于反馈网络而言的，即在网络计算中不存在反馈。3层前馈网络是在输入和输出层之间含有一个隐含层，每层含有多个神经元的前馈网络。BP学习算法是目前最重要的一种神经网络学习算法，在学习过程中，从任意权值 W 出发，计算实际输出 $Y'(t)$ 及其与期望的输出 $Y(t)$ 的均方差 $E(t)$。为使 $E(t)$ 达到最小，要对 W 进行调节。调节方法利用最小二乘法获得，即计算 E 相对于所有权重的 W_{ij} 的微分，如果增加一个指定的权值会使 E 增大，那么就减小此权值，否则就增大此权值。在所有权值调节好了以后，再开始新一轮的计算和调节，直到权重和误差固定为止。

基于前馈神经网络实现CAC的基本原理是：将用户提供的业务量特性参数、要求的QoS参数以及将信元到达速率、信元损失率、信元产生率、干线线路利用率和已接受连接数等交换机复用状态信号作为神经网络的输入，预测的QoS作为神经网络的输出。通过对大量历史数据的学习，计算和调整神经网络的连接权重，便可建立输入与输出之间的一个非线性关系。有了这样的关系，便可根据用户提交的业务量特性、要求的QoS以及当前的交换机复用状态来预测QoS，如果满足要求便可接受连接请求，否则便拒绝。

3）基于遗传算法的路由选择

大多数生物体通过自然选择和有性生殖实现进化。自然选择的原则是适者生存，它决定了群体中哪些个体能够生存和继续繁殖，有性生殖保证了后代基因中的混合和重组。

遗传算法(GA，Genetic Algorithm)是基于自然进化原理的学习算法。在这种算法中，以繁殖许多候选策略，优胜劣汰为基础，进行策略的不断改良和优化。

遗传算法利用简单的编码技术和繁殖机制来表现复杂的现象，解决困难的问题。它不受搜索空间的限制性假设的约束，不要求连续性、单峰等假设，并且它具有并行性，适合于大规模并行计算。

遗传算法在宽带网络的路由选择中得到了应用。一个重要的例子是计算最优组播路由。组播是信息网络中一种传递信息的形式。随着因特网络上各种新业务的普及，这种传递信息的形式变得越来越重要。例如，在发 E-mail 的时候，常常会把一封 E-mail 发向若干个接收者。最优组播路由选择问题可归结为寻找图上最小 Steiner 树问题。将发送者和所有接收者所在的节点称为必须连接的节点，其他节点称为未确定节点，而最终在最小 Steiner 树上的未确定节点称为 Steiner 节点。显然，如果确定了最小 Steiner 树上所有 Steiner 节点，就可以用最小生成树算法(MST，Minimum Steiner Tree)求出最小 Steiner 树，亦即得到了组播的最佳路由。

此外，遗传算法也被用于求解网络的路由选择方案。通常，在网络级确定路由选择方法时应该考虑网络中各条线路上流量的动态均衡和最小时延。这是一个复杂度很高。动态性很强的问题。采用通常的解析方法虽然也能找到最优解的范围或可行解，但算法复杂，实时性难以得到保证。研究表明，遗传算法是解决这一问题的有效方法。

参考文献

[1] 谢希仁. 计算机网络(第 2 版). 北京：电子工业出版社，1999
[2] 谭浩强. 计算机网络教程(第 2 版). 北京：电子工业出版社，2003
[3] 张国鸣，唐树才. 网络管理实用技术. 北京：清华大学出版社，2002

参考网址

[1] www.yesky.com
[2] www.chinaitlab.com
[3] www.ccidnet.com
[4] www.c114.com.cn
[5] www.pconline.com.cn